Gesellschaft für
Reaktorsicherheit (GRS) mbH

Ermittlung der Kriterien
für die Anwendung
systemanalytischer Methoden
zur Durchführung von

Sicherheitsanalysen für Chemieanlagen

U. Hauptmanns
P. Hömke
J. Huber
G. Reichart
H.-G. Riotte

GRS-59

Gesellschaft für
Reaktorsicherheit (GRS) mbH

Ermittlung der Kriterien
für die Anwendung
systemanalytischer Methoden
zur Durchführung von

Sicherheitsanalysen für Chemieanlagen

Ulrich Hauptmanns
Paul Hömke
Josef Huber
Günther Reichart
Hans-Gerhard Riotte

GRS-59 (Dezember 1985)
ISBN 3-923875-07-X

Der vorliegende Bericht wurde im Auftrag des Umweltbundesamtes erstellt. Er ist inhaltsgleich mit dem Forschungsbericht 104 09 267, Luftreinhaltung (Umweltforschungsplan des Bundesministers des Innern), der dem Auftraggeber am 30. September 1984 vorgelegt wurde.

Kurzfassung

Im vorliegenden Bericht wird ein Vorschlag zur Klassifizierung von Chemieanlagen nach dem Gefährdungspotential mit dem Ziel gemacht, diejenigen Produktionszweige zu ermitteln, in denen quantitative Methoden der Sicherheitsbeurteilung sinnvoll eingesetzt werden können. Außerdem werden die üblichen zur Untersuchung der Sicherheit von Chemieanlagen angewandten qualitativen Verfahren kurz vorgestellt. Ihr Einsatz wird an einigen Beispielen aus der Literatur erläutert. Diese Verfahren können auch zur Vorbereitung einer Fehlerbaumanalyse dienen, deren Vorgehensweise ebenso beschrieben wird wie die Methoden zur Ermittlung von Zuverlässigkeitsdaten. Es wird eine Strategie zur Erhebung von Zuverlässigkeitsdaten für die Analyse von Chemieanlagen vorgeschlagen. Ein vorläufiger Referenzdatensatz, der auf Auswertungen im Bereich der Energieerzeugung und Literaturangaben zu Chemieanlagen beruht, wird angegeben. Die Quantifizierung menschlichen Fehlverhaltens bei der Bedienung von Chemieanlagen wird behandelt.

Der praktische Einsatz der Fehlerbaumanalyse ist an einer Untersuchung der Prozeßschritte Nitrierung und Auskochen einer Anlage zur Herstellung des Sprengstoffs Hexogen dargelegt worden. Ihre Anwendung führte auf eine Reihe nutzbringender Vorschläge zur Erhöhung der Anlagensicherheit, die darüber hinaus - obwohl dies nicht das ausdrückliche Ziel der Analyse war - auch eine Erhöhung ihrer Verfügbarkeit bewirken. Manche Ergebnisse resultierten bereits aus den qualitativen Überlegungen, die bei der Erarbeitung der Fehlerbäume angestellt wurden. Die Quantifizierung der Fehlerbäume brachte zusätzliche Einsichten und deckte Bereiche auf, in denen die Sicherheitsvorkehrungen unausgewogen waren. Die aus ihr abgeleiteten Vorschläge führen zu einer erheblichen Erhöhung der Anlagensicherheit und lassen sich mit geringem technischen und finanziellen Aufwand verwirklichen.

Aufgrund des noch bestehenden Mangels an geeigneten Zuverlässigkeitsdaten für Chemieanlagen sollten die Ergebnisse der

Fehlerbaumanalyse auf diesem Gebiet derzeit bevorzugt zum Vergleich von Auslegungsalternativen herangezogen und nicht so sehr als Absolutwerte angesehen werden. Diese Situation könnte durch eine systematische Erhebung von Zuverlässigkeitsdaten verbessert werden. Die Untersuchung zeigte allerdings auch, daß es eine Reihe von sicherheitstechnisch wichtigen Systemen gibt, die nur wenige typisch chemisch belastete Komponenten enthalten. Für solche Systeme liegen auch derzeit schon geeignete Zuverlässigkeitsdaten vor.

Die Untersuchung der Analyse hat gezeigt, daß die Fehlerbaumanalyse ein geeignetes Instrument zur Sicherheitsbeurteilung von Chemieanlagen sein kann. Der Anlagenbetreiber hat die aus der Analyse hervorgegangenen Verbesserungsvorschläge zum größten Teil verwirklicht.

Abstract

A proposal for classifying chemical plants according to their hazard potential is made with the object of finding those branches of production in which it makes sense to use quantitative methods of safety assessment. After that the qualitative methods habitually used for investigating chemical plant safety are presented and their application is explained taking examples from the literature. The methods may serve for preparing a fault tree analysis, whose procedure as well as that for collecting reliability data is explained. A strategy for obtaining reliability data for the analysis of chemical plants is proposed and a preliminary reference data set based on evaluations in the field of energy production and values from the literature on chemical plants is given. The quantification of human failure in handling chemical plants is discussed.

The practical application of fault tree analysis is demonstrated analyzing the process steps nitration and boiling of a plant for the production of the explosive hexogen. Its use has led to a number of useful proposals for increasing plant

safety which, in addition, increase its availability, although this had not been the express aim of the analysis. Some of the results were obtained already from the qualitative considerations required for working out the fault trees. The quantification of the trees brought further insights and uncovered areas of imbalanced safety measures. The proposals derived from the analysis led to a substantial increase of plant safety and may be put into practice at low technical and financial expense.

Owing to the lack of appropriate reliability data still existing for chemical plants the results of fault tree analyses in this field should rather be used for comparing design alternatives than be considered in absolute terms. This situation may be improved by systematically collecting reliability data. On the other hand, the investigation has shown that there are a number of safety relevant systems containing only few components with typically chemical exposure. For such systems appropriate reliability data are already available.

The investigation of the plant has shown that fault tree analysis can be an appropriate instrument for the assessment of chemical plant safety. The plant owner has put into practice the majority of the proposals derived from the analysis.

INHALT

BILDER

TABELLEN

1. EINFÜHRUNG

Seit längerer Zeit werden eine Reihe qualitativer Methoden wie Checklisten, Ausfalleffektanalysen, vorläufige Gefahrenanalysen oder "Hazard and Operability Studies" zur Untersuchung und Verbesserung der Sicherheit von Chemieanlagen verwendet.

In neuerer Zeit wird versucht, auch die vor allem zur Sicherheitsuntersuchung von Kernkraftwerken angewandten Fehlerbaumanalysen zu nutzen. Diese erfordern zunächst ebenfalls eine qualitative Anlagenuntersuchung, erlauben aber dann eine Quantifizierung mit Hilfe von Wahrscheinlichkeiten, weshalb sie auch probabilistische Untersuchungen genannt werden. Die Fehlerbaumanalyse kann zur Untersuchung einzelner technischer Systeme verwendet werden, um deren Verfügbarkeit oder Zuverlässigkeit zu ermitteln, oder sie kann im Rahmen von Risikostudien zur Berechnung der Eintrittshäufigkeiten von Stör- und Unfällen in Gesamtanlagen herangezogen werden. Solche Risikostudien, in denen neben der Eintrittshäufigkeit auch die Schadensfolgen ermittelt werden, sind in der Kerntechnik /1-1/, /1-2/ und auch für Chemieanlagen /1-3/ durchgeführt worden. Während jedoch der Wissensstand in der Kerntechnik bereits eine Abschätzung des mit der Nutzung der Kernenergie verbundenen Risikos erlaubt, hatte die Untersuchung für Chemieanlagen weitgehend das Ziel, die Eignung der genannten Methoden auf diesem Gebiet zu prüfen. Sie wurde grundsätzlich bejaht, wenn auch noch eine Reihe von Problempunkten aufgedeckt wurden. Diese betreffen sowohl die Modellierung der Schadensfolgen als auch die Bereitstellung geeigneter Zuverlässigkeitsdaten für die Quantifizierung der Fehlerbäume.

Analytische Methoden zur Ermittlung der Eintrittshäufigkeiten von Anlagenstörfällen sind insbesondere dann angezeigt, wenn die statistische Erfahrung mit einem bestimmten Anlagentyp nicht ausreicht, um seine Sicherheit zu beurteilen. Dies wird vor allem bei neuartigen Anlagen der Fall sein und bei Systemen, die eine besonders hohe Zuverlässigkeit aufweisen, so daß es einer großen akkumulierten Betriebszeit (Anlagenbetriebs-

zeit x Anlagenzahl) bedarf, um ein statistisch verläßliches Ergebnis zu erzielen. Darüber hinaus gestatten analytische Methoden, Schwachstellen in Anlagen aufzudecken und unterschiedliche Vorschläge zu ihrer Behebung auf ihre Wirksamkeit zu überprüfen. Dies sollte wegen des damit verbundenen Aufwandes jedoch nicht generell erfolgen, sondern nur dann, wenn ein besonderes Gefahrenpotential vorliegt oder mit einer Anlage Neuland beschritten wird. Oftmals wird es auch ausreichen, anstelle der Gesamtanlage nur sicherheitsrelevante Systeme, wie beispielsweise Notabschaltungseinrichtungen, mit Fehlerbaumanalysen zu behandeln, um Schwachstellen herauszufinden und durch deren Beseitigung die Verfügbarkeit im Anforderungsfall zu erhöhen. Bei weniger gefahrenträchtigen Prozessen werden in der Regel qualitative Untersuchungsmethoden ausreichen.

Im Kapitel 2 wird der Versuch einer groben Einteilung der chemischen Industrie nach dem Gefährdungspotential einzelner Herstellungsprozesse unternommen. Im Kapitel 3 werden qualitative Methoden zur Analyse der Sicherheit von Chemieanlagen beschrieben. Daran schließt sich im Kapitel 4 eine Darstellung der Fehlerbaumanalyse an. Das Kapitel 5 ist den speziellen Problemen bei der Erstellung einer Datenbasis für Fehlerbaumanalysen von Chemieanlagen gewidmet. Dabei wird ein vorläufiger Satz von Zuverlässigkeitsdaten angegeben. Außerdem wird die Problematik einer Quantifizierung des menschlichen Fehlverhaltens behandelt. In Kapitel 6 schließlich wird die Vorgehensweise bei einer Fehlerbaumanalyse durch die Untersuchung wesentlicher Bereiche einer Anlage zur Herstellung des Sprengstoffs Hexogen aufgezeigt.

2. ÜBERLEGUNGEN ZUR KLASSIFIZIERUNG VON CHEMIEANLAGEN NACH IHREM GEFAHRENPOTENTIAL

Chemieanlagen können aufgrund physikalischer Betriebsbedingungen, wie extremer Drücke und Temperaturen, und der Eigenschaften der in ihnen vorhandenen Stoffe zu einer Gefährdung für die Umgebung werden. Sie ist möglich durch das Vorkommen von Bränden oder Explosionen oder durch die Freisetzung toxischer Stoffe.

In der chemischen Industrie wird eine Vielzahl gefährlicher Materialien gehandhabt. In /2-1/ werden beispielsweise 13 000 häufig verwendete Chemikalien mit gefährlichen Eigenschaften aufgeführt. Diese werden durch Angaben über eine Reihe von Größen wie Siedepunkt, Flammpunkt, Entzündungstemperatur, Zündbereich, Feuergefährlichkeit, Explosionsgefährlichkeit und Toxizität charakterisiert. Im Dow Index /2-2/ wird die Intensität der Energiefreisetzung durch einen Materialfaktor, der Entflammbarkeit und Reaktivität eines Stoffes beinhaltet, beschrieben. Eine Zusammenfassung gefährdungsträchtiger Stoffeigenschaften bietet der Gefahrendiamant. Bei ihm werden die bereits genannten drei Gefährdungsarten jeweils durch eine Einteilung in fünf Klassen erfaßt, die unterschiedliche Gefährdungsgrade darstellen. Der Gefahrendiamant wird vor allem im Zusammenhang mit dem Transport gefährlicher Stoffe angewendet. In /2-3/ erfolgt beispielsweise auf seiner Grundlage eine Bewertung von mehr als 800 Materialien.

Die genannten Klassifizierungen sind sicherlich eine der Grundlagen zur Beurteilung des Gefahrenpotentials chemischer Prozesse. Eine solche Beurteilung wird allerdings dadurch erschwert, daß nicht nur die mögliche Gefährlichkeit der Ausgangsstoffe und des Reaktionsproduktes zu betrachten ist. Vielmehr kann es insbesondere bei Prozessen für die Herstellung organischer Stoffe zu Nebenprodukten kommen, die gefährlich sein können, selbst wenn die Einsatzstoffe und das Hauptprodukt der Reaktion harmlos sind.

Des weiteren ist daran zu denken, daß an sich ungefährliche Stoffe durch unerwünschte Reaktionen mit Prozeßmedien oder Substanzen aus der Umgebung in gefährliche Stoffe umgesetzt werden können. Werden Prozeßparameter nicht innerhalb der vorgesehenen Toleranzen gehalten, kann die Möglichkeit bestehen, daß sich gefährliche Stoffe bilden, die bei normaler Prozeßführung nicht auftreten.

Ob jedoch das Gefahrenpotential, das den in einem Prozeß vorhandenen Stoffen innewohnt, zu einer konkreten Gefährdung führt, hängt von den physikalischen Parametern, der technischen Auslegung, der Handhabung und Qualitätssicherung bei Erstellung und Betrieb der Anlagen ab, in denen der Prozeß abläuft. Die erwartete Eintrittshäufigkeit für Gefährdungen durch eine Anlage, also ihre Störfalleintrittshäufigkeit, kann im allgemeinen nur durch eine Zuverlässigkeitsanalyse ermittelt werden, da in der Regel die statistische Erfahrung dafür nicht ausreicht. Sollten jedoch solche Analysen zur Grundlage einer Klassifizierung der chemischen Herstellungsprozesse nach ihrem Gefährdungspotential gemacht werden, wäre ein ungeheuerer Aufwand erforderlich, selbst bei der nicht unbedingt zutreffenden Annahme, daß jede analysierte Anlage repräsentativ für eine ganze Klasse ähnlicher Anlagen ist. Hinzu kommen erhebliche Schwierigkeiten bei der Ermittlung des Schadensumfanges, da hier neben Art und Menge der am Störfall beteiligten Stoffe die näheren Umständen des Störfalls eine Rolle spielen und Faktoren wie geographische und meteorologische Gegebenheiten, Aufenthaltsorte von Betriebsangehörigen während des Störfalls und die Bevölkerungsverteilung in der Umgebung der Anlage zu berücksichtigen sind. Diese können nur durch die Entwicklung einer Reihe von Störfallszenarien adäquat erfaßt werden.

Es liegt auf der Hand, daß die oben skizzierte Vorgehensweise, die den bereits erwähnten Risikostudien zugrunde liegt, nur in Einzelfällen angewandt werden kann. Dabei wird es sich vor allem um besonders gefahrenträchtige Prozesse und Anlagen, über die wenig Betriebserfahrung vorliegt, handeln. In allen ande-

ren Fällen sollte die Klassifizierung aufgrund einer groben Beurteilung ausreichen, die sich auf gesammelte Betriebserfahrung stützt, oder sich eines Rasters, wie beispielsweise des Dow-Indexes /2-2/, bedient. Es enthält die Betriebserfahrung in Form von Stoff- und Prozeßparametern, die für das mögliche Auftreten eines Störfalls bedeutsam sind, und faßt diese mit Hilfe eines Wichtungsschemas zu einer Zahl zusammen. Diese Zahl erlaubt eine Einschätzung des Gefährdungspotentials der betrachteten Anlage. Beide Vorgehensweisen werden nachfolgend eingehender geschildert.

Die für die Klassifizierung von Anlagen nach ihrem Gefährdungspotential notwendige Betriebserfahrung findet sich im Grundsatz in Statistiken über Störfälle. Hieraus können Angaben über die Anzahl der Störfälle während eines Zeitraumes, über den betreffenden Herstellungsprozeß und den Schadensumfang entnommen werden.

Wird die Zahl der Störfälle bei einem bestimmten Produktionsprozeß während eines Zeitraums ins Verhältnis zur Gesamtzahl der Störfälle in der chemischen Industrie während desselben Zeitraumes gesetzt, ergibt sich eine Kennzahl, die den relativen Beitrag des betrachteten Produktionsprozesses zum gesamten Unfallgeschehen wiedergibt. Bezeichnet man die Häufigkeit der Störfälle beim Produktionsprozeß i mit H_i und den relativen Beitrag zur Gesamthäufigkeit mit f_i, so läßt sich der Zusammenhang durch folgende Formel darstellen:

$$f_i = \frac{H_i}{\sum_{i=1}^{I} H_i} \qquad (2.1)$$

In der Gleichung (2.1) ist I die Gesamtzahl der Produktionsprozesse, bei denen während des Betrachtungszeitraumes Störfälle auftraten. Berechnet man f_i aus Gleichung (2.1) für eine Reihe von Produktionsprozessen, so läßt sich eine Rangfolge

auf der Grundlage der Eintrittshäufigkeiten aufstellen, in der das Gewicht nicht nur durch die Störfallhäufigkeit der einzelnen Anlagen, sondern auch durch deren Anzahl bestimmt wird; denn

$$H_i = h_i \cdot n_i \qquad (2.2)$$

Dabei ist h_i die mittlere Unfallhäufigkeit des Produktionsprozesses i und n_i die mittlere Anzahl von Anlagen des Types i, die während des Betrachtungszeitraumes betrieben werden. Mit anderen Worten: Der Index ist bereits mit der vorherrschenden Struktur des Sektors Chemie gewichtet, was auch sinnvoll ist.

Eine nach Gleichung (2.1) ermittelte Rangfolge geht davon aus, daß das Schadensausmaß pro Störfall in etwa gleich ist. Sollte dies nicht der Fall sein, sind anstelle der Störfallhäufigkeit die Anzahl von Toten, Verletzten oder das Ausmaß der Sachschäden zugrunde zu legen. Sinnvoll wäre es dabei, alle drei Schadensarten gleichzeitig zu berücksichtigen. Dies würde jedoch Probleme der Wichtung einzelner Schadensarten aufwerfen. Andererseits zielt die Anwendung probabilistischer Methoden darauf ab, die Eintrittshäufigkeit von Störfällen zu verringern, so daß sich die nach Gleichung (2.1) berechneten Kennzahlen anbieten, um einen sinnvollen Einsatzbereich für sie abzustekken.

Die skizzierte Vorgehensweise wurde unter Benutzung der in /2-4/ aufgeführten Daten zu Störfällen und Betriebsstörungen in Chemieanlagen mit Sach- und Personenschäden angewendet. Obwohl die Datensammlung nahezu vollständig ist, sind die Ergebnisse, die in Tabelle 2.1 aufgeführt werden, nur als grobe Näherung zu betrachten.

Dies liegt vor allem an Abgrenzungsschwierigkeiten, da die Unterscheidung zwischen Produktion und Transport nicht immer eindeutig ist und sich manche Störfälle nicht genau einem Produktionszweig zuordnen lassen. Darüber hinaus gehen die Kenn-

Tab. 2.1:

Beiträge einzelner Produktionszweige zu Störfällen im Bereich Chemie auf der Grundlage der Daten aus /2-4/ für die Bundesrepublik Deutschland und Westberlin zwischen 1970 und 1980

Art der Produktion	Anzahl der Ereignisse H_i	Relative Häufigkeit f_i in %	Eintrittshäufigkeit pro Jahr		
			5%-Fraktile	Mittelwert	95%-Fraktile
Sprengstoff	4	11	0,14	0,4	0,92
Polymerisierte Kohlenwasserstoffe	4	11	0,14	0,4	0,92
Schwefelsäure	3	8,3	0,06	0,3	0,78
Mineralöl	3	8,3	0,06	0,3	0,78
Chlor	2	5,6	0,04	0,2	0,63
Phosgen	2	5,6	0,04	0,2	0,63
Harz	2	5,6	0,04	0,2	0,63
Acetylen	1	2,8	0,005	0,1	0,47
Acetylcellulose	1	2,8	0,005	0,1	0,47
Desinfektionsmittel	1	2,8	0,005	0,1	0,47
Diazinon	1	2,8	0,005	0,1	0,47
Dichlorbenzol	1	2,8	0,005	0,1	0,47
Erdgas	1	2,8	0,005	0,1	0,47
Ethylen	1	2,8	0,005	0,1	0,47
Fluorwasserstoff	1	2,8	0,005	0,1	0,47
Imprägniermittel	1	2,8	0,005	0,1	0,47
Klebemittel	1	2,8	0,005	0,1	0,47
Knochenöl	1	2,8	0,005	0,1	0,47
Nitroanisoylchlorid	1	2,8	0,005	0,1	0,47
Pflanzenschutzmittel	1	2,8	0,005	0,1	0,47
Phosphoroxydchlorid	1	2,8	0,005	0,1	0,47
Polyurethan	1	2,8	0,005	0,1	0,47
Schwefelwasserstoff	1	2,8	0,005	0,1	0,47
Summe	$\sum_{i=1}^{I} H_i = 36$	$\sum_{i=1}^{I} f_i = 100$			

zahlen davon aus, daß sich die Produktionsstruktur während des Betrachtungszeitraums nicht verändert, was allerdings nur bedingt zutrifft.

Zugrunde gelegt wurden Störfälle in der Bundesrepublik Deutschland und Westberlin zwischen 1970 und 1980. Diese Eingrenzung wurde vorgenommen, damit nicht technisch veraltete Anlagen und möglicherweise andere Produktionsbedingungen das Ergebnis be-

einflussen. Es wurden nur Ereignisse mit Personenschäden, insgesamt 36, berücksichtigt. Dabei ereigneten sich 43 Todesfälle, von denen 12 bei der Sprengstoffherstellung auftraten. Bei den übrigen Störfällen ist das Schadensausmaß pro Störfall ungefähr gleich groß. Als besonders gefährdungsträchtig erweisen sich Anlagen zur Herstellung von

- Sprengstoffen,
- polymerisierten Kohlenwasserstoffen,
- Schwefelsäure,
- Mineralöl,
- Chlor,
- Phosgen,
- Harzen.

Die genannten Produktionsprozesse sollten Gegenstand detaillierterer Sicherheitsanalysen sein.

Die Anzahl der zugrundegelegten Vorfälle ist insgesamt relativ gering, so daß unter Umständen nicht alle relevanten Stoffe berücksichtigt sind. Eine Erweiterung der statistischen Basis wäre zu erreichen, wenn man den Beobachtungszeitraum ausdehnte und andere Länder zusätzlich berücksichtigte. Dies hätte jedoch den Nachteil, daß - wie bereits erwähnt - möglicherweise technisch veraltete Anlagen einbezogen würden bzw. eine von der Bundesrepublik abweichende Produktionstruktur Einfluß auf die Ergebnisse gewönne[1]). Die vorangehenden Überlegungen zeigen die Grenze der retrospektiven statistischen Betrachtung auf.

Mit Hilfe einer Nullausfallstatistik läßt sich ermitteln, daß für alle diejenigen Herstellungsprozesse, in denen sich kein Störfall ereignet hat, eine Eintrittshäufigkeit für einen Störfall von

---

[1]) Eine Nutzung der ausländischen Erfahrung wäre allerdings über die Ermittlung der Störfallhäufigkeit pro Anlage, h_i, gemäß Gleichung (2.2) möglich. Dazu wäre es aber erforderlich, die Größe der jeweiligen Grundgesamtheit n_i zu kennen. Diese zu erheben, geht über den Rahmen der vorliegenden Arbeit hinaus.

$$H_i < 0{,}3\ a^{-1} \quad (i > I) \quad ^{1)} \tag{2.3}$$

bei einem Vertrauensniveau von 95 % anzusetzen ist.

Erheblich aufwendiger als die Klassifizierung auf der Grundlage von Unfallstatistiken ist die Anwendung eines Rasters. Dies erfordert für typische Anlagen eines jeden Produktionszweiges beispielsweise nach dem Dow-Index /2-2/ die folgenden Erhebungen:

- Gefährliche Stoffeigenschaften
  - oxidierender Stoff,
  - Stoffe, die in Reaktionen mit Wasser brennbare Gase erzeugen,
  - Stoffe, die zu einer spontanen Aufheizung fähig sind,
  - Stoffe, die spontan polymerisieren können,
  - Stoffe, die explosiv zerfallen können,
  - Stoffe, die detonieren können.

- Gefährliche Anlageneigenschaften
  - Be- oder Entladungsvorgänge,
  - Handhabung entflammbarer Stoffe in offenen Systemen,
  - kontinuierliche Prozesse,
  - diskontinuierliche Prozesse,
  - Möglichkeiten von Verunreinigungen,
  - Prozesse bei Unterdruck,
  - Betriebspunkte nahe der Explosionsgrenze,
  - niedrige Temperaturen in Behältern aus kohlenstoffhaltigem Stahl,
  - Betrieb oberhalb des Flammpunktes,
  - Betrieb oberhalb der Zündtemperatur,
  - Betrieb bei hohen Drücken (> 17 bar),
  - schwer kontrollierbare Reaktionen,
  - Möglichkeit der Explosion,
  - große Mengen entflammbarer Flüssigkeiten.

$^{1)}$ $1 - \exp(-H_i T) = 0{,}95$, wobei $T = 10$ a Beobachtungszeit

Zusätzlich können anlagenspezifische Eigenschaften berücksichtigt werden, wobei im Falle guter Auslegung auch eine Minderung des Gefahrenpotentials möglich ist. Bei der voranstehenden Klassifizierung sind Giftstoffe nicht erfaßt.

Eine Anwendung des Dow-Indexes und einiger ähnlicher Methoden auf eine Reihe chemischer Prozesse ist in /2-5/ dokumentiert. Für mögliche toxische Belastungen wird dabei eine getrennte Abschätzung vorgenommen. Da mehrere Verfahren zur Herstellung desselben Stoffes betrachtet werden, läßt sich auch dasjenige mit dem geringsten Gefahrenpotential angeben.

3. METHODEN DER SYSTEMANALYSE

3.1 Allgemeines

Gefährdungs- und Risikoanalysen in der Industrie dienen der systematischen Überprüfung vorhandener oder geplanter Anlagen im Hinblick auf eine Identifizierung und Bewertung potentiell gefährlicher Anlagenzustände sowie möglicher Schadenskonsequenzen. Das Anwendungsspektrum reicht dabei vom Einsatz als Entscheidungshilfe bei der sicherheitstechnischen Verbesserung von Anlagenteilen bis hin zur Unterstützung öffentlicher Entscheidungsprozesse, z.B. bei der geplanten Ansiedlung neuer oder der Erweiterung bereits bestehender Industrieanlagen.

Basis der sicherheitstechnischen Auslegung von Industrieanlagen ist die Erfahrung mit dem geplanten Anlagentyp und dem darin ablaufenden Prozeß. Diese Erfahrung hat in Normen, technischen Regeln und Richtlinien ihren Niederschlag gefunden. Besonders in stark innovativen Industriezweigen, wie z.B. der chemischen Industrie, wird diese Erfahrung durch neue Methoden ergänzt, die ein systematisches Vorgehen zum Erkennen und Bewerten potentieller Gefährdungen erlauben. Diese systematischen Methoden umfassen einfache qualitative Vorgehensweisen zur Identifizierung möglicher Gefahren, aber auch Zuverlässigkeitsuntersuchungen und Risikoanalysen. Sie unterscheiden sich erheblich in bezug auf das Analysenziel, die Vorgehensweise und den Analysenaufwand.

Voraussetzung für die Anwendung systemanalytischer Methoden ist in jedem Fall eine genaue Kenntnis der Anlage und der in ihr ablaufenden Prozesse. Im einzelnen werden in der Regel Angaben zu folgenden Punkten benötigt:

- Anlagen- und Systemaufbau,
- Betriebsbedingungen und betriebliche Abläufe,
- Standort und Umgebung

sowie die insbesondere unter dem Gesichtspunkt der Gefahrenermittlung wesentlichen Daten über

- gefährliche Stoffe,
- Mengenverteilung der Stoffe in der Anlage,
- gefährliche Anlagenzustände,
- vorhandene Sicherheits- und Schutzeinrichtungen.

Die Informationen zu Anlagenaufbau und Standort umfassen eine Beschreibung der Anlage, ihrer Anordnung, der Auslegungs- und Konstruktionsmerkmale von Anlagenteilen, Systemen und Komponenten. Des weiteren werden die Betriebs- und Handhabungsabläufe dargestellt. Außerdem sind Angaben zur Bevölkerungsverteilung in der Umgebung, zur Lage der Schutzzonen und zur Verkehrssituation in der Umgebung erforderlich, falls auch die Schadensfolgen abgeschätzt werden sollen.

Die wichtigsten im Bereich chemischer Industrieanlagen eingesetzten systemanalytischen Methoden werden nachfolgend kurz beschrieben. Im Abschnitt 3.7 wird dann auf einige Anwendungen aus der Literatur beispielhaft eingegangen. Die Fehlerbaumanalyse, die in der vorliegenden Arbeit angewandt wurde, wird im Kapitel 4 getrennt behandelt.

3.2 Gefährdungsindizes

Ein Gefährdungsindex wird durch die Erfassung des gefährlichen Inventars der zu untersuchenden Anlage sowie durch eine Bewertung der Stoffe und des angewandten Produktionsverfahrens mit empirisch gewonnenen Faktoren ermittelt. Die Methodik wurde ursprünglich zu Versicherungszwecken entwickelt und erlaubt durch die Berechnung eines Zahlenwertes das in der betrachteten Anlage vorhandene Gefährdungspotential zu bewerten. Dieser berücksichtigt sowohl die Häufigkeit als auch die Größe einer zur Gefährdung führenden Freisetzung.

Die bekanntesten Gefährdungsindizes sind der "Dow Fire and Explosion Index" /3-1/ und der "Mond Fire, Explosion and Toxicity Index" /3-2/. Für die Berechnung beider Indizes wird die zu betrachtende Chemieanlage in einzelne Bereiche (Grundein-

heiten) aufgeteilt. Für diese Grundeinheiten werden dann Materialfaktoren ermittelt, in die Stoffeigenschaften wie Entflammbarkeit, Reaktivität und beim Mond-Index auch Toxizität eingehen. Diese werden dann nach prozeß- und systemspezifischen Gesichtspunkten gewichtet. Sie umfassen z.B. beim Mond-Index

- die im Prozeß vorhandenen Stoffmengen,
- die Art des Prozesses und den Schwierigkeitsgrad der Prozeßsteuerung,
- Randbedingungen für das Produktionsverfahren,
- die Auslegung des Systems.

Beide Index-Verfahren wurden über ihren ursprünglichen Anwendungsbereich hinaus mehrfach erweitert. So können auch Indizes für Toxizität und ein Gesamtindex für Gefährdungen aus Explosion, Feuer und Toxizität berechnet und eine Abschätzung des maximalen wahrscheinlichen Sachschadens (maximum probable property damage) vorgenommen werden.

Die Gefährdungsindizes werden empirisch ermittelt, wobei auch subjektive Einschätzungen eingehen. Daraus ergeben sich Zahlenwerte zur Beschreibung des Gefährdungspotentials, die jedoch keine absolute Bedeutung haben. Sie erlauben lediglich einen Vergleich mit anderen Indexwerten, die nach derselben Methode für andere Chemieanlagen gewonnen wurden. Dadurch ermöglichen sie einen Vergleich des Gefährdungspotentials verschiedener Anlagen.

3.3 Checklisten

Die Checkliste enthält aus der Erfahrung bekannte Gefahren der verwendeten Prozeßmedien und Versagensmöglichkeiten von Komponenten. Folgendes Beispiel zeigt eine einfache Checkliste für gefährliche Energiequellen (nach /3-3/):

1. Brennstoffe
2. Treibstoffe
3. Zündquellen

4. Geladene elektrische Kondensatoren
5. Akkumulatoren
6. Elektrostatische Aufladung
7. Druckbehälter
8. Federbelastete Teile
9. Hängevorrichtungen
10. Gasgenerator
11. Elektrische Generatoren
12. Radioaktive Energiequellen
13. Fallende Objekte
14. Heizvorrichtungen
15. Pumpen, Gebläse, Ventilatoren
16. Rotierende Maschinen
17. Antriebsvorrichtungen

Checklisten werden angewendet, um einen groben Überblick über Gefährdungspotentiale zu erlangen. Für jede Komponente oder jedes Teilsystem wird dabei anhand der in der Liste enthaltenen Merkposten die Möglichkeit einer Gefährdung abgeschätzt.

Da Checklisten auf Erfahrungen mit den verschiedenen Versagensarten oder potentiellen Gefährdungen beruhen, wurden für verschiedene Industriezweige, wie z.B. Raumfahrt oder chemische Prozeßindustrie, spezifische Checklisten entwickelt /3-2/ /3-3/, die nur teilweise auf andere Systeme übertragen werden können. Eine ausführliche Literaturerhebung über Checklisten findet sich in /3-4/, wo 18 unterschiedliche und in verschiedenen Bereichen angewandte Checklisten aufgeführt werden.

Um die Untersuchung wirkungsvoller zu gestalten, werden Checklisten auch als Fragelisten geführt. Dabei werden die Fragen "offen" formuliert, d.h., sie können nicht einfach mit "ja" oder "nein" beantwortet werden, sondern zwingen zur tieferen Beschäftigung mit den angesprochenen Gefahrenquellen.

Checklisten sind bewußt allgemein gehalten und werden meist nicht in allen ihren Einzelheiten genau auf das zu untersuchende System anwendbar sein. Sie enthalten keinerlei Quanti-

fizierung, so daß sie eine Bewertung verschiedener möglicher Gefährdungen oder geplanter Sicherheits- und Schutzsysteme nicht erlauben.

3.4 Hazard and Operability Study

Das Verfahren der "Hazard and Operability Study" - auch kurz als HAZOP-Verfahren bezeichnet - wurde zuerst in /3-5/ publiziert und später auch als Leitfaden unter dem Titel "A Guide to Hazard and Operability Studies" von der Chemical Industries Association UK veröffentlicht /3-6/. Im deutschsprachigen Raum wurde die Methode in einer Übersetzung als PAAG-Verfahren eingeführt /3-7/. Dabei wird das Ziel des Verfahrens als

> "Anwendung einer strengen, systematischen und kritischen Überprüfung auf Verfahren und Auslegungsziele bei neuen Anlagen, um abzuschätzen, welches Gefährdungspotential durch Fehlbedienung oder Fehlfunktion einzelner technischer Einrichtungen entstehen kann und welche Auswirkungen sich daraus für die gesamte Anlage ergeben können",

beschrieben. Der Grundgedanke des HAZOP-Verfahrens besteht darin, hypothetische Störungen in einem technischen System durch Verwendung bestimmter Leitworte zu erkennen (Tabelle 3.1).

Vom methodischen Ansatz her ist das HAZOP-Verfahren nicht auf Neuanlagen beschränkt. So wird vielmehr in /3-7/ festgestellt, daß HAZOP-Studien an bereits vorhandenen Anlagen zum Beispiel dazu benutzt werden können, Bedienungsmethoden und Betriebsbedingungen zu verbessern.

HAZOP-Studien sind grundsätzlich qualitativ. Ein kleines Team - bestehend z.B. aus Betriebsingenieur, Verfahrenstechniker, Chemiker, Produktionsleiter und Projektleitung - untersucht die vorgeschlagene Auslegung einer Anlage oder eines Anlagenteilbereiches, indem die auslegungsgemäße Funktionsweise von Anlagenteilen in Frage gestellt wird, um daraus möglicherweise

Tab. 3.1:
Leitworte zur Durchführung einer HAZOP-Studie /3-7/

Leitworte	Bedeutungen	Kommentare
NEIN oder NICHT (KEIN oder KEINE)	Die völlige Verneinung dieser Funktion	Kein Teil der Funktionen wird ausgeübt, aber es geschieht auch nichts anderes.
MEHR WENIGER	Quantitativer Zuwachs oder Abnahme	Das bezieht sich auf Mengen und Eigenschaften wie Mengenströme und Temperaturen, aber auch auf Funktionen, wie ERWÄRMEN und REAGIEREN.
SOWOHL ALS AUCH TEILWEISE (ZUM TEIL)	Ein qualitativer Zuwachs Eine qualitative Abnahme	Alle vorgegebenen Funktionen und Betriebsvorgänge werden erreicht. Zusätzlich passiert jedoch auch etwas ANDERES. Nur einige Sollfunktionen werden erreicht, manche nicht.
UMKEHRUNG	Das logische Gegenteil der Soll-Funktion	Das betrifft hauptsächliche Funktionen, z.B. entgegengesetztes Fließen oder entgegengesetzte chemische Reaktion. Es kann auch auf Substanzen angewandt werden, d.h. GIFT anstelle von Gegenmitteln oder D- anstelle von L-optischen Isomeren.
ANDERS ALS	Völliger Austausch	Es wird nicht eine einzige der ursprünglich festgelegten Funktionen ausgeführt. Etwas völlig anderes geschieht.

ergebende Gefahrenzustände aufzudecken. Um die Vorstellungskraft des HAZOP-Teams systematisch anzuregen, geschieht dieses Infragestellen mittels eines Kataloges von Leitworten, wie z.B. "mehr", "weniger" oder "nicht" (Tabelle 3.1), die systematisch auf die Sollfunktion des zu prüfenden Systems angewandt werden, indem beispielsweise bei dem Leitwort "mehr" nach den Auswirkungen eines zu hohen Massenstroms durch einen Anlagenteil gefragt wird. Die Leitworte werden verwendet, um sicherzustellen, daß die Fragen auch wirklich jeden denkbaren Weg aufdecken, auf dem der betrachtete Teil von seiner Sollfunktion abweichen könnte. Auf diese Art werden gewöhnlich eine Anzahl theoretisch möglicher Störfälle aufgedeckt. Jeder Störfall wird dann einzeln untersucht, um herauszufinden, wie er verursacht wird, welche Auswirkungen er haben und durch welche Gegenmaßnahmen er beherrscht oder verhütet werden kann.

In der in /3-7/ publizierten Form ist der Leitworte-Katalog allgemeiner Natur, so daß die Methode sowohl auf große und komplexe Verfahren als auch auf Einzelaggregate, auf kontinuierliche und auf diskontinuierliche Prozesse angewandt werden kann. Um jedoch die Anwendung für weniger erfahrene HAZOP-

Teams zu erleichtern, können die Leitworte auf spezifische Prozesse zugeschnitten werden. So wird in /3-8/ ein Satz Leitworte angegeben, der speziell für die Anwendung bei kontinuierlichen Prozessen entwickelt wurde.

Obwohl zur Beurteilung potentieller Störfälle bei einzelnen Teilbereichen der zu untersuchenden Anlage auch im Rahmen der HAZOP-Studie quantitative Abschätzungen benutzt werden können, besteht das wesentliche Ziel einer HAZOP-Studie darin, mögliche Gefährdungspotentiale aufzufinden und ihre auslösenden Ereignisse zu identifizieren.

3.5 Ausfalleffektanalyse

Das dieser Methode - die im Englischen als Failure Mode and Effect Analysis (FMEA) bezeichnet wird - zugrundeliegende Prinzip besteht darin, alle Komponenten des betrachteten Systems auf mögliche Ausfallarten hin zu untersuchen und die Konsequenzen des Ausfalls zu analysieren /3-9/. Es handelt sich dabei um induktive Vorgehensweise.

Um die Ausfalleffektanalyse auf komplexe Systeme mit vielen Komponenten anzuwenden, wird sie formalisiert und in vier Hauptschritten durchgeführt:

- Erfassung aller einzelnen Komponenten des untersuchten Systems,
- Identifizierung aller möglichen Ausfallarten für jede Komponente,
- Ermittlung von Folgen der Ausfälle unterschiedlicher Art für das Gesamtsystem,
- Bewertung und Vergleich der Eintrittswahrscheinlichkeiten für Ausfälle unterschiedlicher Arten.

Die Ergebnisse der Ausfalleffektanalyse werden normalerweise in Tabellen aufgeführt, die allerdings bei komplexen Systemen und in Fällen, wo Ausfallart und -effekt nicht in direkter Beziehung stehen, sehr unhandlich werden /3-10/. Durch Angabe

der Eintrittshäufigkeit der einzelnen betrachteten Ereignisse kann ein erster Eindruck von deren Bedeutung gewonnen werden.

Ausfalleffektanalysen behandeln im Gegensatz zur Fehlerbaumanalyse nur einzelne Ausfälle und keine Ausfallkombinationen, sie können aber als Vorbereitung einer Fehlerbaumanalyse dienen. Auch wenn sie nicht explizit dargelegt werden, sind Überlegungen nach der Art, wie sie bei der Ausfalleffektanalyse erforderlich sind, implizit in Fehlerbäumen enthalten.

3.6 Ereignisablaufanalyse

In der Ereignisablaufanalyse werden, ausgehend von einem definierten auslösenden Ereignis (z.B. Bruch einer Rohrleitung) und abhängig von Erfolg oder Versagen dann notwendiger Eingriffe von Sicherheitssystemen, die verschiedenen möglichen Auswirkungen dieses Ereignisses ermittelt /3-11/, /3-12/. Je nachdem, welche Gegenmaßnahmen erforderlich und welche Betriebs- und Sicherheitssysteme (Systemfunktion) zur Durchführung dieser Gegenmaßnahmen vorhanden sind, ergeben sich aufgrund des nicht auszuschließenden Versagens der Systemfunktionen Verzweigungen in den möglichen Ereignisabläufen. Diese werden in einem Ereignisablaufdiagramm (Bild 3.1) zusammengefaßt.

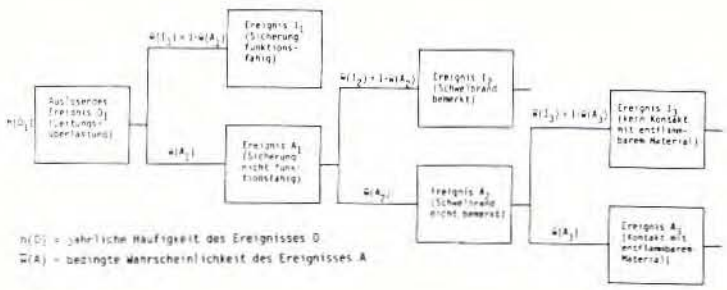


Bild 3.1:
Schematisches Beispiel eines Ereignisablaufdiagramms (aus /3-13/)

Welche Systemfunktionen aufrechterhalten und welche neu angefordert werden, wird durch Simulation des anlagendynamischen Verhaltens festgestellt. Die Simulation stützt sich auf mathematische Modelle für physikalische oder chemische Vorgänge. Jeder Zweig des Ereignisablaufdiagramms ist die statische Beschreibung eines in der Zeit kontinuierlich ablaufenden Vorganges. Dieser wird durch einige wenige Punkte dargestellt, bei denen in Abhängigkeit vom Funktionieren oder Versagen der angeforderten Systemfunktion über den weiteren Verlauf des Prozesses entschieden wird.

Die Ereignisablaufanalyse läßt sich in zwei Teilaufgaben gliedern, und zwar

- in die systemtechnischen Untersuchungen, die sich mit dem Ereignisablauf beschäftigen, soweit er durch das erfolgreiche Eingreifen der Betriebs- und Sicherheitssysteme bestimmt wird, und
- in die Untersuchungen, die den weiteren, aus einem angenommenen Versagen von Betriebs- und Sicherungssystemen resultierenden Ereignisablauf innerhalb der Anlage bis hin zur Freisetzung von Schadstoffen und Energien behandeln.

In die Ereignisablaufdiagramme für die erste Teilaufgabe werden alle Verzweigungen der Ereignisabläufe aufgenommen, die aufgrund der physikalischen und chemischen Untersuchungen oder sich verändernder Anforderungen an die Betriebs- und Sicherheitssysteme von Bedeutung sein könnten. Dabei wird sich im allgemeinen der binären Logik bedient, d.h., Systeme werden entweder als voll funktionsfähig oder voll ausgefallen betrachtet und mögliche Zwischenzustände einem der beiden Zustände - in der Regel dem Ausfall - zugeordnet.

Bei der praktischen Durchführung der Ereignisablaufanalyse ist auf folgendes sorgfältig zu achten:

- Es können Abhängigkeiten von Systemfunktionen untereinander bestehen. Dies kann die Folge davon sein, daß die Gegenmaßnahmen bei Eintreten eines auslösenden Ereignisses vielfach von Systemen durchgeführt werden, die nicht unabhängig von-

einander sind. Die Anforderungen an die Systemfunktionen hängen dabei vom jeweils betrachteten Ereignisablauf und von Art und Umfang des auslösenden Ereignisses ab.

- Es können systembedingte Folgeausfälle auftreten. Der Aufbau der Ereignisabläufe, d.h. die Kette der aufeinanderfolgenden Ereignisse, entspricht generell dem zeitlichen Ablauf des Störfalles. Dabei müssen bei jedem der aufeinanderfolgenden Ereignisse die Folgen der vorausgehenden Ereignisse berücksichtigt werden. Würde z.B. durch Wasser, das aus einem Leck austritt, ein Meßfühler eines Schutzsystems funktionsunfähig, so wäre dies bei später erforderlichen Maßnahmen zu berücksichtigen.

3.7 Anwendungsbeispiele aus der Literatur

3.7.1 Vorgehensweisen beim Erkennen und Bewerten inhärenter Gefahrenpotentiale

Eine Möglichkeit zur Bewertung des Gefahrenpotentials einer Chemieanlage bieten der Dow- und der Mond-Index. Ihre Anwendung erfordert eine genauere Analyse der Anlage. Deshalb ist die Ermittlung der Indizes zu aufwendig, um sie routinemäßig zur Bewertung des Gefahrenpotentials einzusetzen. Dies ist jedoch oft auch nicht notwendig, da für eine grobe Klassifizierung, beispielsweise im Hinblick auf die Notwendigkeit von Sicherheitsanalysen für eine Anlage, eine Ermittlung ihres Inventars an gefährlichen Stoffen ausreichen kann. Ein solches Verfahren wird in Großbritannien angewandt, wo für verschiedene gefährliche Stoffe ein Grenzinventar angegeben wird, bei dessen Überschreiten eine Sicherheitsüberprüfung der Anlage durch das "Health and Safety Executive" erfolgt /3-14/.

Ein ähnliches Vorgehen zur Identifizierung von Anlagen mit größerem Gefährdungspotential ("major hazard") wird in den Niederlanden entwickelt, wobei Grenzwerte für die Inventare verschiedener chemischer Substanzen und für die Gefährdungskategorien "brennbar toxisch", "extrem toxisch" und "explo-

siv" angegeben werden /3-15/. Bei der Festlegung der Grenzwerte werden die Substanzen unter bestimmten Referenzbedingungen betrachtet, beispielsweise "eingesetzt in einem chemischen Prozeß", "in der flüssigen Phase vorliegend", "bei Umgebungstemperatur vorliegend oder darüber". Bei Anlagen, in denen Schadstoffe unter anderen als den Referenzbedingungen vorliegen, werden Korrekturfaktoren angewandt. Diese können beispielsweise berücksichtigen, ob der Schadstoff im Freien oder innerhalb von Gebäuden gehandhabt wird, in welchem Aggregatzustand er sich befindet, ob er in einem chemischen Prozeß eingesetzt oder nur gelagert wird.

3.7.2 Identifizierung unerwünschter Ereignisse

Bei Chemieanlagen sind aufgrund der häufig vorhandenen zahlreichen Stoffe unterschiedlicher Gefährdungsart, der unterschiedlichen Stoffumsetzungen und Prozeßabläufe oft eine größere Anzahl unerwünschter Ereignisse zu betrachten. Zu ihrer Identifizierung können die qualitativen Methoden der Systemanalyse eingesetzt werden. Sie erfordern einen erheblich geringeren Aufwand als quantitative Methoden. Ihre Anwendung ist daher weiter verbreitet.

Einen Vergleich zweier der hierzu in Frage kommenden Methoden bietet die Rijnmond-Studie /3-16/, in der zum Auffinden der unerwünschten Ereignisse sowohl die Checklisten-Methode (Abschnitt 3.3) als auch das HAZOP-Verfahren (Abschnitt 3.4) eingesetzt werden. Dabei zeigte sich, daß mit dem HAZOP-Verfahren nur wenige auslösende Ereignisse zusätzlich zu denen, die mit Checklisten gefunden wurden, entdeckt werden konnten. Dies wird unter anderem darauf zurückgeführt, daß

- aufgrund der Zielsetzung der Studie nur Ereignisse mit schweren Auswirkungen (zwei oder mehr Tote) betrachtet werden sollten und
- sich die Studie mit relativ einfachen Anlagen befaßt, für die weltweit viele Jahre Betriebserfahrung als Grundlage für die Checkliste vorliegt.

Eine Kombination von Checkliste und HAZOP-Verfahren wurde auch bei der Analyse einer Offshore-Bohrinsel nach der Richtlinie des Norwegian Petroleum Directorate angewandt /3-17/. Dabei konnten in der Entwurfsphase annähernd 200 unerwünschte Ereignisse identifiziert werden. Für die Untersuchung mit der Checkliste wurde die Anlage in unterschiedliche räumliche Bereiche aufgeteilt, während bei Anwendung des HAZOP-Verfahrens Anlagenteile und Systeme entsprechend ihrem funktionellen Zusammenhang gegliedert wurden.

Bei bestimmten Anwendungen, beispielsweise wenn es nur um Abschätzungen von Gefährdungen geht, kann die Aufstellung einer Checkliste relativ trivial sein. So können bei Gefährdungsanalysen von Schiffsverladestellen die zu betrachtenden Ereignisse, wie Kollision, Auf-Grund-Laufen, spontanes Behälterversagen, die zu einer Freisetzung der Ladung mit gefährlichen Stoffen führen, sofort angegeben werden /3-18/.

Zur Identifizierung potentieller Schadensereignisse bei komplexen Anlagestrukturen kann auch die Ausfalleffektanalyse (Abschnitt 3.5) eingesetzt werden. Sie wurde in /3-19/ bei der Untersuchung einer Offshore-Schiffsanlage zur Verflüssigung von Erdgas und seiner Lagerung angewandt. Ziel der Analyse war es, schon im Entwurfsstadium der Anlage diejenigen kritischen Bereiche für die Auslegung und den Betrieb zu identifizieren, in denen Ausfälle von Systemen und Komponenten wegen Gasaustritt oder LNG-Leckagen flüssigen Erdgases (Liquid Natural Gas/LNG) die Sicherheit der Anlage beeinträchtigen könnten. Es zeigt sich, daß viele der mit der systematisch durchgeführten Ausfalleffektanalyse untersuchten Ausfälle hinsichtlich der Fehlereffekte unbedeutend waren. Für den Anlagenbereich "Versagen der druckführenden Umschließung" konnten sechs unerwünschte Ereignisse identifiziert werden. Die zugehörigen Ausfallkombinationen wurden mit Fehlerbaummethoden analysiert. Der Umfang derjenigen Auslegungsfehler, die mit HAZOP-Studien hätten aufgedeckt werden können, wird in /3-19/ auf 57 % geschätzt.

Einen Anhaltspunkt zur Beurteilung des Leistungsvermögens der qualitativen Methoden der Gefährdungsanalyse bietet der Vergleich von Anlagenanalysen nach verschiedenen Verfahren mit Unfällen, die zuvor in diesen Anlagen aufgetreten, aber unbekannt waren. In /3-20/ werden dazu als Fallstudien u.a. ein Explosionsunglück während des Trocknens von Nitrozellulose-Pulver und das Bersten eines Nitroanilin-Reaktors behandelt. Im Falle des Explosionsunglückes wird festgestellt, daß bei Analysen mit Hilfe allgemein üblicher Checklisten die tatsächlich zum Unfall führenden Ereignisse nicht erkannt und Folgefehler sowie Bedienungsfehler nicht erfaßt werden. Zur Verbesserung dieser Verfahren wird empfohlen, Fallstudien auszuwerten und Checklisten aufgrund früherer Unfälle zu überarbeiten. Darüber hinaus wird die parallele Anwendung mehrerer Verfahren zur Gefährdungsidentifizierung vorgeschlagen. Da neben Komponentenfunktionen (z.B. "Ventil öffnet") auch Systemzustände (z.B. "Luftzufuhr vorhanden") in den Fehlerbaum aufgenommen wurden, konnte der zum Unfall führende Versagenspfad durch die Fehlerbaumanalyse "vorhergesagt" werden. Der Fall des Berstens eines Nitroanilin-Reaktors ist besonders typisch für ein chemisches Gefährdungspotential, da hier eine durchgehende (exotherme) Reaktion für die Gefährdung ausschlaggebend war. Dazu wird ausgeführt, daß weder durch eine "Hazard and Operability"-Studie noch durch die Anwendung der Fehlerbaumanalyse das eingetretene Behälterversagen erfaßt worden wäre. Es hätte hierzu insbesondere einer besseren Kenntnis der Reaktionskinetik möglicher unerwünschter Reaktionen sowie der Entwicklung analytischer Methoden bedurft, mit denen solche Reaktionen systematischer hätten behandelt werden können.

In einem ähnlichen Vorgehen wird in /3-21/ für 215 Fälle untersucht, inwieweit durch eine Anwendung des HAZOP-Verfahrens später aufgetretene Sicherheitsprobleme bereits bei der Auslegung von Chemieanlagen hätten entdeckt werden können.

4. FEHLERBAUMANALYSEN

4.1 Allgemeines

Bei der Untersuchung der Zuverlässigkeit großer technischer Systeme hat sich die Fehlerbaumanalyse bewährt. Zu ihrer Durchführung wird ein unerwünschtes Ereignis (z.B. den Ausfall der Kühlung oder die Freisetzung gefährlicher Stoffe) vorgegeben und nach allen dazu führenden Ursachen gesucht. Im allgemeinen ergeben sich dabei eine Vielzahl von Ausfallkombinationen jeweils mehrerer Komponenten[1]), die zum Ausfall von Teilsystemen führen. Der Ausfall eines Teilsystems kann das unerwünschte Ereignis entweder direkt oder in Kombination mit Ausfällen anderer Teilsysteme zur Folge haben.

Die Fehlerbaumanalyse ermöglicht durch die Darstellung komplexer Zusammenhänge in den Systemen mit Hilfe der binären Logik, die nur das Funktionieren bzw. den Ausfall von Komponenten kennt[2]), und durch eine geeignete grafische Darstellung eine übersichtliche Behandlung selbst bei großen technischen Systemen. Dabei lassen sich auch spezifische Probleme, wie z.B. Folgeausfälle, menschliches Fehlverhalten und Common-Mode-Ausfälle (Abschnitt 5.4), berücksichtigen. Der Fehlerbaum ist mithin eine logische Darstellung der Verknüpfungen zwischen den Ausfällen der Komponenten und dem unerwünschten Ereignis. Dabei werden im allgemeinen "UND"- und "ODER"-Gatter benutzt. Beim "UND"-Gatter müssen alle Eingangsereigniss erfüllt sein, damit das Ausgangsereignis zutrifft, während beim "ODER"-Gatter jedes einzelne der Eingangsereignisse allein oder aber zusammen mit anderen das Ausgangsereignis hervor-

---

[1]) Der Begriff Komponente bezeichnet hier sowohl technische Komponenten im eigentlichen Sinne als auch Verfahrensvorschriften und Personen, die in den Betrieb der Anlage eingreifen.

[2]) In letzter Zeit sind auch Ansätze einer Logik mit mehr als zwei Zuständen bekanntgeworden /4-1/, /4-2/, die aber wegen der Schwierigkeiten, zutreffende Ausfallraten für Zwischenzustände zu finden und deterministische Aussagen über das Anlagenverhalten als Folge von teilweisem Komponentenversagen zu machen, keine praktische Bedeutung erlangt haben.

ruft. Bild 4.1 enthält die entsprechenden grafischen Darstellungen und andere in Fehlerbäumen verwendete Sinnbilder.

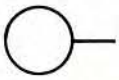
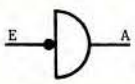
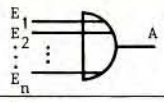
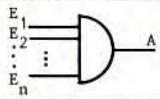
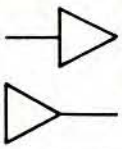
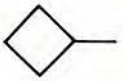
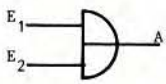
Benennung und Bildzeichen		Bemerkungen
Standardeingang		Das Bildzeichen steht für einen Funktionselementausfall, wenn primäres Versagen möglich ist.
NICHT-Verknüpfung		Die NICHT-Verknüpfung steht für die Negation. Ist der Eingang E der Verknpüfung "0", so ist der Ausgang A "1" und umgekehrt.
ODER-Verknüpfung		Die ODER-Verknüpfung steht für die logische Vereinigung. Der Ausgang A ist "1", wenn mindestens einer der Eingänge E_i "1" ist.
UND-Verknüpfung		Die UND-Verknüpfung steht für den logischen Durchschnitt. Der Ausgang A ist "1", wenn alle Eingänge $E_1,\ldots,E_n$ "1" sind.
Kommentar		Beschreibungen von Eingängen bzw. Ausgängen von Verknüpfungen werden in Rechtecke eingetragen.
Übertragungsausgang Übertragungseingang		Mit einem Übertragungsbildzeichen wird der Fehlerbaum abgebrochen bzw. an anderer Stelle fortgesetzt.
Sekundäreingang		Das Bildzeichen wird als ein Eingang der SEKUNDÄR-Verknüpfung verwendet.
SEKUNDÄR-Verknüpfung		Die SEKUNDÄR-Verknüpfung steht für das Entstehen eines Sekundärausfalls aus einem Primärausfall. Ändert sich E_1 von "0" nach "1", so wird mit einer durch den Sekundäreingang E_2 angegebenen Wahrscheinlichkeit und Dauer der Ausgangszustand A der Verknüpfung von "0" nach "1" geändert.

Bild 4.1:

Darstellung der wichtigsten Sinnbilder für Fehlerbäume (aus /4-3/)

Die Fehlerbaumanalyse ist ein vollständiges Verfahren, d.h., aufgrund der deduktiven Vorgehensweise liefert sie bei konsequenter Anwendung im Prinzip alle Ereigniskombinationen, die zum unerwünschten Ereignis führen. Grenzen sind nicht vom Verfahren her, sondern nur durch Kenntnis und Sorgfalt des Anwenders gesetzt. Selbstverständlich kann eine Fehlerbaumanalyse keine Phänomene aufdecken, die zum Zeitpunkt der Analyse unbekannt sind.

Fehlerbaumanalysen werden entweder zur Ermittlung der Zuverlässigkeit einzelner Systeme verwendet, wie auf dem Gebiet der Chemieanlagen beispielsweise in /4-4/, /4-5/, /4-6/, /4-7/, oder im Rahmen von Risikostudien /4-8/, /4-9/ und /4-10/, in denen eine Vielzahl von Systemen mit ihrer Hilfe untersucht wird. Insbesondere bei Analysen auf dem Gebiet der Kerntechnik dienen sie dazu, die Eintrittswahrscheinlichkeiten der Verzweigungen in den Ereignisablaufdiagrammen (Abschnitt 3.6) zu ermitteln. Bei den erwähnten Untersuchungen treten Fehlerbäume auf, die wegen ihrer Größe im allgemeinen nur mit Hilfe von EDV-Anlagen ausgewertet werden können. Die dabei verwendeten Rechenprogramme bedienen sich simulativer oder analytischer Verfahren.

Bei den simulativen Verfahren kann noch zwischen der direkten Simulation von Zuverlässigkeitsparametern und der simulativen Ermittlung von Minimalschnitten unterschieden werden. Die analytischen Verfahren berechnen ebenfalls die Minimalschnitte des Fehlerbaums.

4.2 Minimalschnitte

Als Minimalschnitt eines Systems wird eine Kombination von Komponenten bezeichnet, deren gemeinsamer Ausfall gerade ausreicht, einen Systemausfall zu bewirken. Mathematisch gesprochen handelt es sich um eine notwendige und hinreichende Bedingung für einen Systemausfall. Im allgemeinen gibt es für ein technisches System mehrere Minimalschnitte. Jeder von ihnen stellt eine mögliche Art des Systemversagens dar.

Die Zerlegung eines Fehlerbaums in seine Minimalschnitte gibt Auskunft über die logische Struktur des betrachteten Systems. Auf diese Weise ist es möglich, festzustellen, welche Komponenten allein oder im Verbund mit anderen das System zum Versagen bringen können (Minimalschnitte aus einer oder mehreren Komponenten) oder an wievielen Versagensarten (Minimalschnitten) eine Komponente beteiligt ist. Diese Information bildet die Grundlage für eine Schwachstellenanalyse des Systems, da beispielsweise Minimalschnitte, die nur aus einer einzigen Komponente bestehen, das Fehlen von Redundanzen anzeigen. Um Versagenswahrscheinlichkeiten für das System zu ermitteln, bildet man mit Hilfe der Minimalschnitte seine Strukturfunktion[1]). In die Strukturfunktion werden dann die Komponenten-Versagenswahrscheinlichkeiten eingesetzt /4-11/.

Die Versagenswahrscheinlichkeit wird hier über einen Umweg berechnet, der aber u.a. den Vorteil hat, daß dabei zusätzlich die Ausgangsinformationen für die Schwachstellenanalyse geliefert werden. Außerdem lassen sich Kenngrößen für unterschiedliche Zeitpunkte durch Einsetzen von Wahrscheinlichkeiten, die für den betreffenden Zeitpunkt gelten, in die bereits bestimmte Strukturfunktion ermitteln, die somit nur einmal zu berechnen ist.

4.3 Simulative (Monte Carlo) Verfahren

4.3.1 Direkte Bestimmung von Zuverlässigkeitsparametern

Mit Hilfe von Zufallszahlen wird die fiktive Lebensdauer der einzelnen Komponenten des zu untersuchenden technischen Systems auf der Grundlage der zugehörigen Ausfallraten λ berechnet (Kapitel 5). Auf diese Weise wird das Komponentenverhalten nachgebildet, das ursprünglich zu den beobachteten Werten von λ geführt hat. Die fiktive Lebensdauer der einzelnen Komponen-

---

[1]) Die Strukturfunktion ist eine Funktion, die das Versagen oder Funktionieren eines Systems in Abhängigkeit vom Versagen oder Funktionieren seiner Komponenten mathematisch beschreibt.

ten wird mit dem Zeitpunkt T verglichen, für den die Ausfallwahrscheinlichkeit ermittelt werden soll. Alle Komponenten, deren Lebensdauer kürzer ist als das Intervall (0, T), sind ausgefallen. Komponenten, deren Verhalten durch Nichtverfügbarkeiten p beschrieben wird, gelten als ausgefallen, wenn die gezogene Zufallszahl kleiner als p ist.

Anschließend wird eine logische Funktion, die den Fehlerbaum darstellt, abgefragt, um festzustellen, ob aufgrund der ausgefallenen Komponenten ein Systemausfall eintritt oder nicht. Dann wird der Vorgang wiederholt, wobei neue Zufallszahlen gezogen werden und im allgemeinen andere Komponenten ausfallen als bei den vorangegangenen Durchläufen.

Nach einer gewissen Anzahl von Durchläufen, auch Spiele genannt, wird die Ausfallwahrscheinlichkeit für den Zeitpunkt T als Quotient (Anzahl der Ausfälle) : (Gesamtzahl der Spiele) ermittelt. Andere Parameter werden in ähnlicher Weise berechnet /4-12/.

Da das Ergebnis eine Zufallsvariable ist, lassen sich nur Vertrauensbereiche für den wahren Wert des Parameters angeben. Die Größe der Vertrauensbereiche nimmt mit steigender Anzahl an Spielen ab. Die Anzahl der Spiele, die für eine bestimmte Genauigkeit erforderlich ist, hängt vom Kehrwert des Quadrates der Ausfallwahrscheinlichkeit ab und kann bei zuverlässigen Systemen sehr schnell zu aufwendig werden. Eine gewisse Abhilfe können dann varianzreduzierende Methoden schaffen, deren Anwendung jedoch mangels genauer Vorschriften für die Bestimmung der dabei zu verwendenden Gewichtsfaktoren problematisch ist.

4.3.2 Bestimmung von Zuverlässigkeitsparametern über die simulative Ermittlung von Minimalschnitten

Die Ermittlung von Minimalschnitten mit Hilfe der Monte-Carlo-Methode erfolgt nach dem im vorangehenden Abschnitt aufgezeigten Schema. Jeder Systemausfall wird durch den Ausfall mehrerer

Komponenten bewirkt. Unter Umständen kann das System allerdings mehr als die für den Ausfall verantwortlichen Komponenten enthalten. Die überzähligen müssen deshalb herausgenommen werden, damit die verbleibende Menge einen Minimalschnitt darstellt.

Da im vorliegenden Fall nicht direkt Zuverlässigkeitsparameter errechnet, sondern nur Struktureigenschaften des Systems ermittelt werden, läßt sich die Notwendigkeit der großen Anzahl von Spielen für zuverlässige Systeme dadurch umgehen, indem die Bezugszeit T künstlich so festgesetzt wird, daß ungefähr bei der Hälfte der Spiele ein Systemausfall eintritt /4-13/. Es macht sich die Tatsache zunutze, daß technische Systeme ohne Wartung mit zunehmender Betriebszeit immer unzuverlässiger werden.

Die Monte-Carlo-Simulation findet allerdings im allgemeinen nicht sämtliche Minimalschnitte eines Systems, sondern nur diejenigen, die einen wesentlichen Anteil an der Systemunzuverlässigkeit haben. Diese Eigenschaft kann dann erwünscht sein, wenn ein System eine große Anzahl von Minimalschnitten aufweist (dies können u.U. mehrere Millionen sein), deren vollständiges Auffinden an Speicherplatz- und Rechenzeitbegrenzungen scheitern würde.

4.4 Analytische Verfahren

Im Gegensatz zu der im vorangehenden Abschnitt vorgestellten Methode finden analytische Verfahren sämtliche Minimalschnitte eines Systems. Sie bedienen sich dabei Operationen der Booleschen Algebra und benötigen im Gegensatz zur Monte-Carlo-Methode keinerlei Information über das Komponentenverhalten. Diese wird erst bei der probabilistischen Auswertung der Minimalschnitte erforderlich. Bei Fehlerbäumen, die auf sehr viele Minimalschnitte führen, erfordern sie die Festlegung eines Abschneidekriteriums, damit keine Schwierigkeiten aufgrund zu hohen Speicherplatzbedarfs und zu langer Rechenzeiten auftreten. Bezüglich weiterer Einzelheiten des Verfahrens, das in mehreren Varianten verwendet wird, sei auf /4-14/ verwiesen.

4.5 Vergleich der Methoden

Die Methode der direkten Simulation ist ein flexibles Verfahren zur Behandlung komplexer Systeme, wobei beispielsweise Wartungsstrategien, Beschränkungen bezüglich der Reparaturkapazität oder die Inbetriebnahme von Reservesystemen leicht berücksichtigt werden können. Andererseits sind die Ergebnisse nur innerhalb gewisser Vertrauensgrenzen angebbar. Deren Einengung erfordert bei sehr zuverlässigen Systemen eine große Anzahl von Spielen. Die Einschränkungen, die dadurch der Methode auferlegt sind, können durch die Anwendung varianzreduzierender Methoden nur unter bestimmten Bedingungen abgebaut werden.

Die Methoden, die auf der Verwendung der Minimalschnitte beruhen, vermitteln eine tiefere Einsicht in die Systemstruktur. Sie liefern exakte Lösungen oder erlauben, falls Vereinfachungen erforderlich werden, eine genaue Abschätzung des Fehlers. Andererseits lassen sich Wartungsstrategien nur vereinfacht oder unter großem mathematischen Aufwand berücksichtigen. Systeme, deren Fehlerbäume viele Minimalschnitte aufweisen, können - wie bereits erwähnt - insbesondere bei analytischen Verfahren zu Problemen führen. Leider gibt es derzeit keine allgemeine Regel, die angibt, welche Verfahrensweise die geeignete bei der Auswertung eines vorgelegten Fehlerbaums ist. Aus diesem Grunde ist es empfehlenswert, für die praktische Arbeit sowohl über ein Programm zur direkten Simulation von Zuverlässigkeitsparametern als auch über ein Programm, das auf der Ermittlung von Minimalschnitten beruht, zu verfügen.

5. ZUVERLÄSSIGKEITSDATEN UND AUSFALLWAHRSCHEINLICHKEITEN

5.1 Allgemeines

Das Verhalten von Komponenten wird bei der probabilistischen Analyse eines Systems mit Hilfe von Ausfallwahrscheinlichkeiten und Nichtverfügbarkeiten beschrieben. Dabei werden auch Verfahrensvorschriften und Personen, die in den Betrieb eingreifen, als Komponenten behandelt. Jeder Funktion einer Komponente des zu untersuchenden Systems wird ein unabhängiges Funktionselement zugeordnet. Darüber hinaus kann auch zur Beschreibung von Common-Mode-Ausfällen (CMA) (Abschnitt 5.4), d.h. dem gemeinsamen Ausfall mehrerer redundanter Komponenten, ein einziges Funktionselement verwendet werden.

Das Ausfallverhalten eines Funktionselementes läßt sich auf eine der beiden folgenden Arten beschreiben /5-1/:

- durch die Ausfallrate λ

  Unter der Ausfallrate wird die relative Abnahme des Bestandes an noch nicht ausgefallenen Funktionselementen verstanden, die pro Zeiteinheit eintritt.

- durch eine Ausfallwahrscheinlichkeit pro Anforderung p

  Unter der Ausfallwahrscheinlichkeit pro Anforderung wird die Wahrscheinlichkeit dafür verstanden, daß bei Anforderung des Funktionselementes ein Ausfall vorliegt, die Komponentenfunktion also in dem vor der Anforderung liegenden Zeitraum ausgefallen ist oder spätestens zum Anforderungszeitpunkt ausfällt.

Beide Größen sind Erfahrungswerte. Sie werden durch statistische Auswertungen von Beobachtungen ermittelt, die beim betrieblichen Einsatz in vergleichbaren technischen Anlagen gemacht werden und einen Mittelwert aus dem Verhalten mehrerer Komponenten eines Typs für die Ausfallrate λ bzw. die Nichtverfügbarkeit p liefern. Im allgemeinen sind beide Größen nicht konstant, sondern hängen von der Zeit ab, wie nachfol-

gend am Beispiel von λ näher erläutert wird. Der zeitliche Verlauf der Ausfallrate läßt sich in der Regel durch eine "Badewannenkurve" (Bild 5.1) beschreiben.

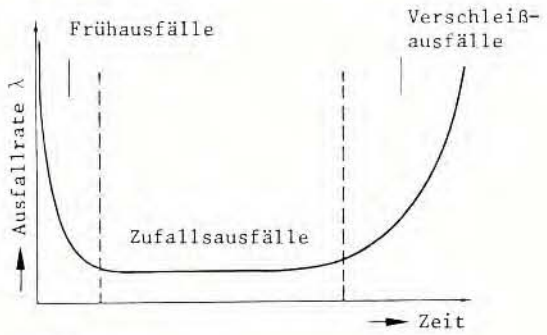


Bild 5.1:
Zeitverhalten der Ausfallrate

Zu Beginn des betrieblichen Einsatzes besteht die Möglichkeit von sogenannten Frühausfällen aufgrund von Fehlern, z.B. aus der Fertigung, die trotz Qualitätssicherung und Inbetriebnahmeprüfungen nicht entdeckt wurden und zu einer erhöhten Ausfallrate führen. Die Zahl derartig fehlerhafter Komponenten nimmt mit fortschreitender Zeit aufgrund von Reparaturen oder durch Austausch ab, bis nur noch Komponenten eines Qualitätsniveaus übrigbleiben. Am Ende der Lebensdauer der Komponenten kann die Ausfallrate infolge von Verschleißausfällen und Alterung zunehmen. Während des wesentlichen Teiles der Einsatzzeit wird das Ausfallverhalten jedoch nicht von systematischen, sondern von zufälligen Fehlern bestimmt; es kann dann mit einer konstanten Ausfallrate gerechnet werden. Diese Zufallsausfälle werden durch eine Exponentialverteilung beschrieben, d.h., die Verteilungsfunktion der Ausfallwahrscheinlichkeit q(t) einer Komponentenfunktion in Abhängigkeit von der Einsatzzeit t ist durch

$$q(t) = 1 - \exp(-\lambda t), \quad t > 0 \tag{5.1}$$

gegeben.

Obwohl dem Auftreten von Früh- und Verschleißausfällen durch Verwendung betriebsbewährter Komponenten, Qualitätskontrollen und Wiederholungsprüfungen entgegengewirkt wird, ist eine Zeitabhängigkeit der Ausfallrate oder -wahrscheinlichkeit über die gesamte Einsatzzeit nicht auszuschließen. Aus der Betriebserfahrung erhält man im allgemeinen Mittelwerte über die gesamte Einsatzzeit für die Ausfallraten bzw. -wahrscheinlichkeiten. Diese konstanten Werte werden in Zuverlässigkeitsanalysen verwendet[1]).

Daten beziehen sich in der Regel auf unabhängige Ausfälle von Komponenten. Da für die Common-Mode-Ausfälle nur in beschränktem Umfang Informationen vorliegen, sind meistens spezielle Zuverlässigkeitsanalysen notwendig, um ihren Einfluß abzuschätzen. Eine besondere Stellung nimmt das menschliche Fehlverhalten ein, bei dem Zuverlässigkeitsabschätzungen für unterschiedliche Handlungen erforderlich sind, die als Funktionselemente in die Fehlerbaumanalyse eingehen; dies wird in Abschnitt 5.5 gesondert behandelt.

Neben dem Ausfallverhalten der Komponenten ist auch ihre Nichtverfügbarkeit infolge von Instandhaltungen zu berücksichtigen. Darunter sind Instandsetzungen, d.h. die Reparatur ausgefallener Komponenten, Wartungen, d.h. regelmäßig vorbeugende Maßnahmen, und Inspektionen, z.B. regelmäßige Funktionsprüfungen, zu verstehen.

Vom Zeitpunkt des Ausfalls bis zum Abschluß der Instandhaltung ist eine Komponente als ausgefallen anzusehen. Bei der theoretischen Behandlung der Instandhaltung werden im allgemeinen folgende Gesichtspunkte berücksichtigt:

- die Häufigkeit der Funktionsanforderungen bzw. der zeitliche Abstand zwischen den regelmäßigen Funktionsprüfungen

---

[1]) Die Berücksichtigung der Zeitabhängigkeit der Ausfallrate ist möglich, führt jedoch zu einem erhöhten Rechenaufwand. In der Regel liegen allerdings doch nur Erfahrungswerte für konstante Ausfallraten vor.

(Inspektionen) und deren Staffelung bei nicht selbstmeldenden Ausfällen;
- sofortige Instandsetzung, sobald ein Ausfall erkannt wird;
- Einstufung einer Komponente als neuwertig nach durchgeführter Instandhaltung.

Sind für das Funktionieren eines Systems verschiedene Funktionsweisen einer Komponente wichtig, so sind die zugehörigen unterschiedlichen Ausfallarten zu berücksichtigen, d.h., in die Fehlerbaumanalyse gehen unterschiedliche Funktionselementausfälle einer Komponente ein. Diese Ausfälle werden oft näherungsweise als voneinander unabhängig betrachtet.

Instandsetzungen von Komponenten können aufgrund eines Ausfalles, der zu Betriebsstörungen führt, erforderlich werden. Darüber hinaus erfolgen sie auch bei Ausfällen, die den Anlagenbetrieb nicht stören, oder im Rahmen der vorbeugenden Wartung. Während solcher Instandsetzungen kann es nötig sein, die Komponente vorübergehend auszubauen oder freizuschalten, so daß sie ihre Funktion nicht mehr ausführen kann. Erfolgt eine solche Instandsetzung während des Betriebs der Anlage, so vermindert sie die Verfügbarkeit der Systemfunktion.

Eine große Zahl verschiedener Instandhaltungsstrategien läßt sich mit Hilfe der Erneuerungstheorie oder der Theorie der Markoff-Prozesse mathematisch behandeln /5-2/. Auf sie wird hier nicht näher eingegangen. Es sei nur noch auf ein Modell zur Beschreibung der periodischen Wartung hingewiesen, das eine einfache Erweiterung der Beziehung (5.1) darstellt /5-3/ und unter folgenden Bedingungen gilt:

- Die Lebensdauer der Komponente wird durch eine Exponentialfunktion beschrieben.
- Das Wartungsintervall ist konstant.
- Ausfälle werden nur bei der Wartung entdeckt.
- Die Reparaturdauer ist klein gegenüber der mittleren Komponentenlebensdauer.
- Nach jeder Wartung ist die Komponente "so gut wie neu".

Unter den genannten Voraussetzungen erhält man für die Nichtverfügbarkeit der Komponente

$$u(t) = 1-e^{-\lambda\cdot(t-n\cdot\theta)};(t > 0),\ (n = 0,1,\ \ldots) \qquad (5.2)$$

In der Gleichung (5.2) ist λ die Ausfallrate der Komponente, θ die Zeit zwischen zwei Wartungen und n der ganze Teil des Quotienten t/θ. Die Beziehung führt zur sogenannten Sägezahnkurve, die schematisch in Bild 5.2 dargestellt ist.

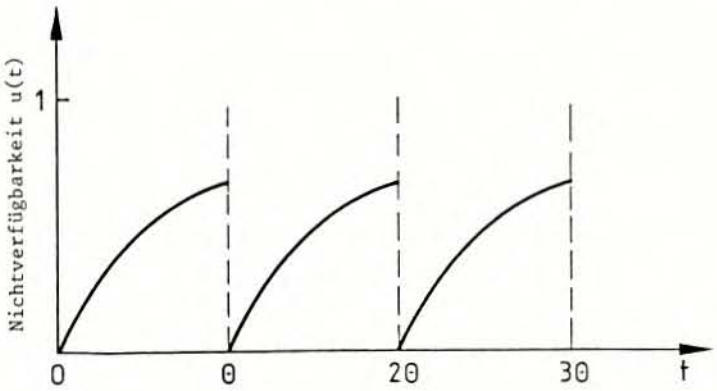


Bild 5.2:
Zeitabhängige Nichtverfügbarkeit einer Komponente bei periodischer Wartung

Durch Integration des Ausdrucks (Gl. 5.2) über das Zeitintervall und Division durch θ erhält man die zeitlich gemittelte Nichtverfügbarkeit einer Komponente

$$\bar{u} = \frac{1}{\theta}\left[\theta + \frac{1}{\lambda}\left(\exp(-\lambda\cdot\theta) - 1\right)\right] \qquad (5.3)$$

Das Ergebnis (Gl. 5.3) läßt sich bei $\lambda\theta << 1$ durch Taylorentwicklung der Exponentialfunktion und Abbruch mit dem dritten Glied vereinfachen, so daß man

$$\bar{u} \sim \frac{\lambda\theta}{2} \qquad (5.4)$$

erhält. Die zeitlich gemittelten Nichtverfügbarkeiten wurden in der im Kapitel 6 dargestellten Analyse auf der Grundlage der Beziehung (Gl. 5.2) durch numerische Integration ermittelt.

5.2 Ausfallraten für Komponenten in Chemieanlagen

Ausfallraten für die Analyse einer Anlage sollten von Komponenten stammen, die den zu bewertenden ähnlich sind und unter vergleichbaren Bedingungen eingesetzt werden. Dies läßt sich bei der Analyse von Chemieanlagen derzeit nicht verwirklichen /5-4/, und es verbleibt nur die Möglichkeit eines Rückgriffs auf Daten aus der Literatur. Dabei ist jedoch die Übertragbarkeit in der Regel zweifelhaft. Der Versuch einer Anpassung der Werte an die zu betrachtende Situation mit Umgebungsfaktoren /5-5/, die in der vorliegenden Arbeit Medieneinflußfaktoren genannt werden, kann nur als Notbehelf gelten.

Eine Literaturdurchsicht führte im wesentlichen auf drei Arbeiten (/5-6/, /5-7/, /5-8/) mit eigenen Daten für Chemieanlagen. Diese sind zusammen mit Angaben aus Auswertungen der GRS, (/5-9/, /5-10/), die - falls erforderlich - unter Benutzung von Medieneinflußfaktoren und ingenieurmäßigen Einschätzungen an die allgemeinen Betriebsbedingungen in Chemieanlagen angepaßt wurden, zu einem vorläufigen Ausfallratensatz verarbeitet worden, der in der Tabelle 5.1 enthalten ist.

Die Ausfallraten wurden dabei als Stichprobe aus einer logarithmischen Normalverteilung betrachtet /5-1/, deren Wahrscheinlichkeitsdichtefunktion folgendermaßen lautet:

$$f(\lambda) = \frac{1}{\sqrt{2\pi}\,s} \exp\left[\frac{(\ln\lambda - \mu)^2}{2\,s^2}\right] \quad (\lambda > 0) \qquad (5.5)$$

Tab. 5.1:

Ausfallraten für Komponenten in Chemieanlagen

Komponente/Operation	Betriebsmedium	Mittelwert in 10^{-6} h^{-1}	Streu-faktor	Bemerkungen
*Ausfall eines Endschalters		2,0	4	Streufaktor geschätzt
*Drehzahlmesser mit Alarm fällt hoch oder niedrig aus		12,7	5	Streufaktor geschätzt
*Ausfall eines Elektromotors		20	3	Streufaktor geschätzt
*Keilriemenriß		17	3	Streufaktor geschätzt
*Automatische Umschaltung		3,0	4	Streufaktor geschätzt
*Versagen eines elektrischen Druckknopfes		0,5	3	Streufaktor geschätzt
*Schalter eines Motors schaltet nicht ab		1,0	4	Streufaktor geschätzt
*Ausfall eines pneumatischen Temperaturalarms		9,5	4,2	
*Ausfall eines magnetischen Vorsteuerventils		31,7	4,5	
*Ausfall eines pneumatischen Reglers		43,6	1,5	
pH-Messer		1578	5,0	Wert aus /5-6/
Gas-Flüssig-Chromatograph		3204	2,0	Wert aus /5-6/
O_2-Analysator		676	6,2	Wert aus /5-6/
CO_2-Analysator		1199	4,0	Wert aus /5-6/ Streufaktor geschätzt
Infrarotanalysator		160	4	Wert aus /5-6/ Streufaktor geschätzt
*ODER-Schaltglied mit 5 Eingängen versagt		0,37	3,0	Wert aus /5-1/
*Startversagen Elektromotor		5,4	3,0	Eigener Wert Streufaktor geschätzt
*Ausfall eines Niveaualarms	Wasser + Feststoffgemisch	195	5	Geschätzt
*Pneumatisches Regelventil öffnet nicht	Wasser + Feststoffgemisch	57	3,6	Mit Medieneinflußfaktor 2 gegenüber Wasser abgeschätzt
*Ausfall eines Niveaureglers	Wasser + Feststoffgemisch	195	5	Geschätzt
*Handabsperrventil öffnet nicht	Wasser + Feststoffgemisch	0,5	3,2	Mit Medieneinflußfaktor 2 gegenüber Wasser abgeschätzt
*Dreiwegeventil schaltet nicht um	Wasser + Feststoffgemisch	195	5	Geschätzt
*Kapazitiver Niveauregler versagt	Wasser + Feststoffgemisch	5,7	4	Streufaktor geschätzt
*Ausfall einer Druckölversorgung	Hydrauliköl	8	10	Geschätzt
*Ausfall eines Ölhydraulikmotors	Hydrauliköl	1	10	Geschätzt
*Ausfall der Druckluftversorgung	Luft	64	3	Streufaktor geschätzt
*Ausfall einer Kühlmaschine	Frigen	210	3	Streufaktor geschätzt
Leitfähigkeitsmessung (bei Flüssigkeiten)		1906	4	Wert aus /5-6/ Streufaktor geschätzt
Leitfähigkeitsmessung (für Wasser in Feststoffen)		1632	4	Wert aus /5-6/ Streufaktor geschätzt
Härtemessung für Wasser		1244	4	Wert aus /5-6/ Streufaktor geschätzt
H_2-Analysator		113	4	Wert aus /5-6/ Streufaktor geschätzt
H_2O-Analysator (Gasphase)		913	4	Wert aus /5-6/ Streufaktor geschätzt

Mit * versehene Werte werden für die in Kapitel 6 beschriebene Untersuchung verwendet und in Abschnitt 6.3 im einzelnen behandelt.

Tab. 5.1: (Fortsetzung)

Komponente/Operation	Betriebsmedium	Mittelwert in 10^{-6} h^{-1}	Streufaktor	Bemerkungen
Thermometer (örtlich) mit Schutzrohr	unerheblich	2,9	2	Eigener Wert und Wert aus /5-6/
*Ausfall eines Alarms über Durchflußmesser	Wasser	28,3	5,8	
*Betriebsversagen einer Pumpe einschließlich Ansteuerung	Wasser	44,4	1,9	
*Startversagen einer Pumpe einschließlich Ansteuerung	Wasser	13,4	3,2	
*Rückschlagklappe schließt nicht bzw. öffnet nicht	Wasser	0,5	6	
*Ausfall Thermostatschalter oder Temperaturwächter einschließlich Alarm	Wasser	3,6	2,2	
*Ausfall Druckwächter einschließlich Abschaltung oder Alarm	Wasser	9,53	4,2	
*Pneumatisches Regelventil regelt nicht	Wasser	28,7	3,6	
*Handabsperrventil läßt sich nicht öffnen	Wasser	0,25	3,2	
*Ausfall eines schwimmergesteuerten Ventils	Wasser	190	5	Geschätzt
*Handregelventil regelt nicht	Wasser	12,3	3	Streufaktor geschätzt
*Motorventil versagt	Wasser	13,2	2	Streufaktor geschätzt
Schwimmerschalter	Wasser	8,1	3	Streufaktor geschätzt
Füllstandsregler (direkte Messung)	Wasser	31,8	4	Streufaktor geschätzt
Differenzdruck für Niveau (linearer Differenzdruckmeßumformer)	Wasser	37,5	3	Streufaktor geschätzt
Radizierender Druckmeßumformer für Durchflußmessung	Wasser	34,1	3	Streufaktor geschätzt
*Ausfall Temperaturmessung mit Widerstandsthermometer in Schutzrohrausführung	Säure bei Umgebungstemperatur	3,5	6	Streufaktor geschätzt
*Betriebsausfall einer Pumpe	Säure bei Umgebungstemperatur	178	1,9	Mit Medieneinflußfaktor 4 gegenüber Wasser abgeschätzt
*Startausfall einer Pumpe	Säure bei Umgebungstemperatur	54	3,2	Mit Medieneinflußfaktor 4 gegenüber Wasser abgeschätzt
*Rückschlagklappe schließt nicht oder öffnet nicht	Säure bei Umgebungstemperatur	2,0	6	Mit Medieneinflußfaktor 4 gegenüber Wasser abgeschätzt
*Ausfall eines kapazitiven Niveaumessers einschließlich Alarm oder Abschaltsignal	Säure bei Umgebungstemperatur	20	2,2	
*Ausfall eines Durchflußmessers mit Rotameter	Säure bei Umgebungstemperatur	115	6	Streufaktor geschätzt
*Absperrventil mit pneumatischem Antrieb öffnet nicht	Säure bei Umgebungstemperatur	3,0	6	Geschätzt
*Bruch einer Welle	Säure bei Umgebungstemperatur	0,2	10	Geschätzt
*Absperrventil mit pneumatischem Antrieb öffnet nicht	Säure bei 50 - 100 °C	6,0	6	Geschätzt
*Ausfall eines Temperaturschalters	Säure bei 50 - 100 °C	14	6	Streufaktor geschätzt, mit Medieneinflußfaktor 4 gegenüber Wasser abgeschätzt
*Bruch einer Welle	Säure bei 50 - 100 °C	0,4	10	Geschätzt
*Ausfall eines Druckwächters mit Schalter oder Alarm	Korrosive Gase	19	4,2	
*Motorventil klemmt	Korrosive Gase	16	3	Streufaktor geschätzt
*Betriebsausfall einer Pumpe	Wasser + Feststoffgemisch	88	1,9	Mit Medieneinflußfaktor 2 gegenüber Wasser abgeschätzt
*Startausfall einer Pumpe	Wasser + Feststoffgemisch	26	3,2	Mit Medieneinflußfaktor 2 gegenüber Wasser abgeschätzt

Mit * versehene Werte werden für die in Kapitel 6 beschriebene Untersuchung verwendet und in Abschnitt 6.3 im einzelnen behandelt.

Für die Anwendung der Verteilung benötigt man die Parameter μ, den Mittelwert der Logarithmen der Ausfallraten, und s^2, die zugehörige Varianz. Sie werden wie folgt geschätzt:

$$\mu = \frac{1}{N} \sum_{n=1}^{N} \ln \lambda_n = \ln \lambda_{50} \qquad (5.6)$$

Dabei ist N die Gesamtzahl der vorhandenen Meß- oder Literaturwerte für die Ausfallrate und λ_{50} der Median der Ausfallraten. Für die Varianz der Logarithmen der Ausfallraten ergibt sich

$$s^2 = \frac{1}{N-1} \sum_{n=1}^{N} (\ln \lambda_n - \mu)^2 \qquad (5.7)$$

Die Streuung der Daten läßt sich durch folgenden Faktor darstellen:

$$K = \exp(s \cdot 1{,}645) \qquad (5.8)$$

In Gleichung (5.8) ist K, auch Unsicherheitsfaktor genannt, so gewählt, daß die Ausfallrate mit einer Wahrscheinlichkeit von 90 % in das Intervall $[\lambda_{50}/K, \lambda_{50} \cdot K]$ fällt, wobei sie mit einer Wahrscheinlichkeit von jeweils 5 % unterhalb der unteren bzw. oberhalb der oberen Intervallgrenze liegt. Lagen mehrere Werte für die Ausfallraten vor, so wurden die Gleichungen (5.6) bis (5.8) zur Ermittlung des Faktors K verwendet. In allen anderen Fällen wurde K aufgrund ingenieurmäßiger Beurteilung geschätzt.

Zwischen den genannten Verteilungsparametern und dem Mittelwert der Verteilung besteht die folgende Beziehung:

$$\lambda = \lambda_{50} \cdot \exp(s^2/2) \qquad (5.9)$$

Es ist offensichtlich, daß die Benutzung der Daten nur mit größter Vorsicht erfolgen sollte und daß eigentlich für die Bewertung des Komponentenverhaltens in Chemieanlagen Ausfallraten in Abhängigkeit von wesentlichen Einflußparametern, wie Temperatur, Druck, Art des Mediums etc., vorliegen müßten. Diese würden es dann erlauben, geeignete Ausfallraten unter Berücksichtigung der Betriebsbedingungen in der betrachteten Anlage auszuwählen. Im folgenden Abschnitt wird deshalb eine Strategie für die Erhebung von Zuverlässigkeitsdaten vorgeschlagen, die den genannten Anforderungen gerecht werden.

5.3 Strategie für eine Datenerhebung in der chemischen Industrie

5.3.1 Notwendigkeit und Ziele einer Datenerhebung

Bei der Auswahl von Zuverlässigkeitsdaten für probabilistische Untersuchungen von Chemieanlagen muß auf Werte aus anderen Bereichen - insbesondere dem Kraftwerksbereich - zurückgegriffen werden. Dabei stellt sich die Frage nach der Übertragbarkeit und den ihr zugrunde liegenden Kriterien. Die Arbeiten zur Bereitstellung einer gesicherten Datenbasis für die Kraftwerkstechnik (/5-9/ bis /5-12/) zeigen, daß hierfür insbesondere die Einflüsse auf das Ausfallverhalten bekannt sein müssen, weil der Idealzustand für die Übertragbarkeit - es liegt eine Beobachtung der exakt gleichen Komponente unter genau den gleichen Betriebs- und Einsatzbedingungen vor - praktisch nicht vorkommt. Sind jedoch die Einflüsse auf das Ausfallverhalten, ihre Abhängigkeit und die Bandbreite der Ergebnisse bekannt, so läßt sich eine geeignete Ausfallrate aus vorliegendem Datenmaterial auswählen und der zugehörige Unsicherheitsfaktor K angeben. Eine Datenerhebung muß mithin die folgenden Ziele haben:

- Ermittlung derjenigen Einflußgrößen auf das Ausfallverhalten, wie z.B. Konstruktion, Werkstoff, Betriebs- und Einsatzbedingungen, Umgebungsbedingungen, Art der Instandhal-

tung usw., die einen signifikanten Einfluß auf die Zuverlässigkeitskenngrößen haben;

- Bereitstellung von Zuverlässigkeitskenngrößen, die entsprechend dem erstgenannten Ziel spezifiziert sind.

Eine Datenerhebung, die diese beiden Ziele erfüllt und weitgehende Vollständigkeit beanspruchen will, erfordert einen hohen Arbeits- und Zeitaufwand.

Da die Aussagekraft probabilistischer Analysen über Störfallrisiken aus Chemieanlagen in großem Maße von qualifizierten Daten abhängt, ist eine Datenerhebung in der Chemie zur Ermittlung spezifizierter Aussagen über das Ausfallverhalten von Komponenten und Systemen notwendig. Neben der Nutzung solcher Daten für probabilistische Analysen existieren eine Reihe weiterer Anwendungsmöglichkeiten für betriebliche Zwecke, wie z.B. die Auswahl der jeweils günstigsten Komponente für den jeweiligen Einsatzort, die Planung von Wartungsmaßnahmen, von vorbeugender Instandsetzung und von Überwachungs- und Prüfzyklen. Dies zeigen Erfahrungen aus anderen Bereichen der Technik. Mit Hilfe der Daten lassen sich Instandhaltungs- und Prüfstrategien optimieren und damit Kosten sparen, ohne die Sicherheit einzubüßen.

Es ist möglich, für die Datenermittlung ein abgestuftes Konzept vorzusehen, mit dem in den Bereichen, in denen die Datenbasis besonders unsicher ist, angefangen und zunächst versucht wird, die Bandbreite von Einflüssen zu bestimmen und durch Daten zu belegen. Im folgenden werden einige Voraussetzungen für eine Datenerhebung angegeben und eine Erhebungsstrategie vorgeschlagen.

5.3.2 Voraussetzungen für eine Datenerhebung im Betrieb

Die Erfahrungen bei der Datenermittlung zeigen, daß es notwendig ist, sich bei der Erfassung der Schäden auf ein betrieblich vorhandenes Informationssystem zu stützen /5-12/, /5-13/.

Die Schadensdaten sollten schon aus betrieblichen Gründen aufgeschrieben werden und für jeden Schaden mindestens die genaue Zuordnung zu dem ausgefallenen Betriebsmittel, der Komponente und dem betroffenen System, das Datum des Schadenseintritts, die Art des Schadens und der Reparatur vorliegen. Rückschlüsse auf Ausfallwirkung, Ausfallart, Art der Fehlerentdeckung, Ausfallursache sowie Dauer der Reparatur sollten möglich sein. Da je nach Art der Beanspruchung auch die Betriebszeiten und Schalthäufigkeiten von Einfluß sind, ist es wünschenswert, daß die entsprechenden Betriebsstunden bzw. Schaltspiele mit Hilfe von Zählern ermittelt werden können, da anderenfalls zu Schätzungen gegriffen werden muß.

Für die zu beobachtenden Anlagenteile muß eine vollständige Liste der Komponenten und Betriebsmittel mit den wesentlichen technischen Daten sowie den betrieblichen Beanspruchungen vorliegen oder erstellt werden.

Wie bei Kraftwerken ist auch bei Chemiebetrieben davon auszugehen, daß ein Auftragswesen eingeführt ist, das wesentliche Teile der benötigten Daten bereits enthält, weil diese auch für betriebliche Zwecke, wie beispielsweise Instandhaltungs- und Ersatzteilplanung, benötigt werden.

5.3.3 Strategie für eine Datenerhebung

Es ist sinnvoll, in der ersten Phase der Erhebung mit einer beschränkten Anzahl von Komponenten die wesentlichen Einflußparameter auf deren Verhalten zu identifizieren und soweit möglich die Bandbreite der Ergebnisse zu bestimmen. Dadurch kann man den Aufwand zunächst geringer halten und sich später auf die genauere Verifizierung der wesentlichen Einflußparameter konzentrieren. Darüber hinaus gelangt man bereits in einer ersten Phase zu einer Datenbasis, auch wenn diese noch nicht sämtliche Anforderungen an Vollständigkeit und Genauigkeit erfüllt.

Als Grundlage für die Auswahl von Typ und Anzahl der zunächst zu beobachtenden Komponenten können diejenigen Einflußgrößen auf Zuverlässigkeitsdaten dienen, die aus der bisherigen Erfahrung bekannt sind, nämlich

- Bauart, Konstruktion,
- Einsatzarten,
- Betriebseinflüsse, insbesondere das Medium,
- Umgebungseinflüsse (nur in manchen Fällen).

Obwohl die Anzahl der Einflußparameter bei Erhebungen für Komponenten in Chemieanlagen wahrscheinlich über die bei Kraftwerken zugrunde gelegten hinaus erweitert werden muß, wird es eine Reihe von Komponenten geben, die von gleicher Bauart sind wie diejenigen, die in der Kraftwerkstechnik eingesetzt werden und unter vergleichbaren Betriebsbedingungen arbeiten. Von ihnen ist ähnliches Ausfallverhalten zu erwarten. Für diese Gruppe von Komponenten wird deshalb zunächst nur eine Kontrollgruppe zu beobachten sein, um eine Absicherung der aus dem Kraftwerksbereich bekannten Daten für mögliche Anwendungen im Sektor Chemie zu erreichen.

Komponenten, die sich nach Technik und Bauart von Kraftwerkskomponenten unterscheiden, sowie solche, die unter dem Einfluß von Betriebs- bzw. Prozeßmedien stehen und nur in der Chemie vorkommen, sollten beobachtet werden. Dabei werden im ersten Ansatz unter den möglichen Prozeßanlagen diejenigen ausgewählt, die aufgrund der Erfahrung des Betriebspersonals weitgehend störungsfrei oder besonders störungsanfällig sind, und solche, die zwischen diesen beiden Extremen liegen. Die Entscheidung über die Zuordnung einer Anlage zu diesen drei Kategorien läßt sich anhand der aus der Vergangenheit vorliegenden Instandhaltungsaufträge vornehmen, wenn eine Statistik über Reparaturaufträge geführt oder entsprechende Aufschreibungen vorgenommen werden. Das Datenerhebungsprojekt sollte dann die folgenden Arbeitspunkte enthalten:

- Analyse der Aufschreibungen von Betriebserfahrungen hinsichtlich ihrer Eignung für eine Erhebung von Zuverlässig-

keitskenngrößen; Erarbeiten von Vorschlägen für eine Ergänzung von Daten und für die Einführung eines Erfassungssystems;

- Entwicklung eines angepaßten Erfassungssystems mit Verschlüsselungen, Formularen, Datenbank und Rechenprogramm;
- Auswahl einiger Prozesse für die Erfassung, in denen für die chemische Industrie typische Beanspruchungen und Komponentenbauarten auftreten;
- Erfassung der relevanten Beanspruchungsmerkmale für die ausgewählten Komponenten und Betriebsmittel sowie der zugehörigen Schadensfälle und Ausfälle sowie Abspeicherung in der Datenbank;
- Auswertung der erfaßten Daten in bezug auf Einflußgrößen für das Ausfallverhalten, Berechnung von Ausfallraten und Reparaturzeiten, spezifiziert nach Einflußgrößen und Ausfallraten; Bereitstellung von qualitativen und quantitativen Angaben über Ausfallursachen, -wirkungen, -entdeckung und Reparaturen.

Die erfaßten und ermittelten Daten können nicht nur für Analysen des Störfallverhaltens, sondern, wie bereits erwähnt, auch für Zwecke der Instandhaltungsoptimierung, der Kostenüberwachung und der Entwurfsüberprüfung verwendet werden.

5.4 Common-Mode-Ausfälle

Über voneinander unabhängige Funktionsausfälle von Komponenten hinaus ist in einem technischen System mit dem Auftreten voneinander abhängiger Funktionsausfälle zu rechnen /5-14/, /5-15/. Besonders unangenehm können diese Ausfälle werden, wenn sie redundante Komponenten betreffen und gleichzeitig oder in einem eng begrenzten Zeitintervall so auftreten, daß die ausgefallenen Zustände gleichzeitig vorliegen. Es wird dann von "Common-Mode-Ausfällen" (CMA) oder "gemeinsam verursachten Ausfällen" gesprochen /5-15/.

Folgende Arten von CMA können unterschieden werden:

- Funktionsausfälle von zwei oder mehr ähnlichen oder baugleichen redundanten Komponenten oder Teilsystemen aufgrund einer gemeinsamen äußeren Ursache. Sie werden als CMA oder "Common Cause Failures" im engeren Sinn bezeichnet.
- Funktionsausfälle von zwei oder mehr redundanten Komponenten oder Teilsystemen, die als Folge eines einzigen Funktionsausfalls auftreten. Sie werden als Folgeausfälle, Sekundärausfälle oder "Causal Failures" bezeichnet.
- Funktionsausfälle von zwei oder mehr redundanten Komponenten oder Teilsystemen, die sich aufgrund von funktionellen Abhängigkeiten, d.h. unmittelbar aus dem Systemaufbau ergeben. So können beispielsweise funktionelle Abhängigkeiten von einem gemeinsamen Hilfssystem, von einer gemeinsamen Ansteuerung oder von einer menschlichen Fehlhandlung bestehen.

Um in Zuverlässigkeitsuntersuchungen für ein bestimmtes vorliegendes System eine möglichst adäquate Wahrscheinlichkeitsbewertung von CMA zu erreichen, sollten gemeinsame Ausfälle redundanter Komponenten wegen funktioneller Abhängigkeiten durch eine detaillierte Fehlerbaumanalyse soweit wie möglich erfaßt werden.

Ebenso sollten Folgeausfälle, sofern sie nicht durch räumliche Anordnung oder durch entsprechende Konstruktion ausgeschlossen werden können, möglichst bereits in die Fehlerbaumanalyse eingehen (z. B. Folgeausfälle aufgrund von fliegenden Bruchstükken, schlagenden Rohrleitungen oder aufgrund von Feuchtigkeit). Es verbleibt dann der Anteil der CMA aufgrund einer gemeinsamen äußeren Ursache (Planungs-, Herstellungs- oder Instandhaltungsfehler, z. B. ungeeignetes Schmiermittel in den Pumpenlagern). Dieser sollte möglichst mit Hilfe von Betriebserfahrung bewertet werden.

Bei diesen CMA im engeren Sinn ist zu differenzieren zwischen solchen, die

- nur bei einem Störfall auftreten oder entdeckt werden,
- bei regelmäßigen Funktionsanforderungen (im Rahmen von Funktionsprüfungen oder anderen regelmäßigen Systemanforderungen) entdeckt werden,
- selbstmeldend sind.

Die Betriebserfahrung liefert in erster Linie Daten für die beiden zuletzt angeführten Arten von CMA, die während des bestimmungsgemäßen Betriebs entdeckt werden. Die nur bei einem Störfall auftretenden oder entdeckbaren CMA können im wesentlichen nur analytisch ermittelt werden. Zu solchen CMA kann es aber nur kommen, wenn die Anforderungen sowohl beim Betrieb als auch bei Funktionsprüfungen nicht repräsentativ für die Anforderungen von Komponenten bzw. Systemen unter Störfallbedingungen sind.

Auch für die während des Betriebs und bei Funktionsprüfungen entdeckbaren CMA erweist sich die Quantifizierung als sehr schwierig, da Beobachtungen nur in geringem Maße dafür heranziehbar sind. Das hat folgende Gründe:

- Nur ein Bruchteil der Komponentenausfälle sind CMA.
- Die Ursachen aufgetretener Ausfälle, die als CMA erkannt werden und einen großen Einfluß auf die Zuverlässigkeit des Systems haben, werden behoben. Gleichartige Ausfälle werden daher nur mit reduzierter Wahrscheinlichkeit wieder auftreten.

Reicht die Betriebserfahrung zur Quantifizierung der CMA nicht aus, so wird versucht, Modelle einzusetzen. Die Modelle zur Bewertung von CMA werden in /5-14/ eingehend beschrieben. Dabei wird insbesondere auf

- die Kopplung von Ausfällen,
- die Beta-Faktor-Methode und
- das spezialisierte Marshall-Olkin-Modell

eingegangen. Die Anwendbarkeit und die Grenzen dieser Modelle werden im folgenden diskutiert.

Die Kopplung von Ausfällen wurde zuerst in WASH-1400 /5-15/ angewandt. Die Verwendung der Methode zur Abschätzung der Wahrscheinlichkeit für den Ausfall der Reaktorschnellabschaltung wurde bereits in /5-16/ heftig kritisiert. Ebenso wurde in /5-14/ darauf hingewiesen, daß sich bei stark redundanten Systemen eine Mittelung über viele Größenordnungen ergibt, so daß dieses Modell dann auf keinen Fall benutzt werden sollte.

Bei der Beta-Faktor-Methode /5-17/ wird davon ausgegangen, daß ein fester Anteil aller Komponentenausfälle, z.B. 10 %, CMA sind, und versucht, dies anhand von Betriebserfahrungen zu belegen. Die Beta-Faktor-Methode ist in /5-14/ ausführlich kommentiert. Ein β-Faktor von 10 %, der für alle Typen von Komponenten gelten soll, wurde auf der Grundlage der früher in der amerikanischen Kernkraftwerkstechnik allgemein üblichen vermaschten 1v2-Systeme ermittelt. Der β-Faktor bewertet dabei auch funktionelle Abhängigkeiten und mangelhafte räumliche Trennung mit. Hingegen wird nicht berücksichtigt, daß mit einer zunehmenden Zahl von redundanten Teilsystemen bzw. Komponenten die Wahrscheinlichkeit eines Systemausfalls abnimmt. Der Einfluß von administrativen Maßnahmen und personeller Redundanz auf die Wahrscheinlichkeit von CMA wird nicht bewertet /5-18/. Auswertungen von β-Faktoren für Chemieanlagen sind nicht bekannt.

Grundsätzlich besteht die Möglichkeit, das Beta-Faktor-Modell redundanzabhängig zu formulieren und den redundanzabhängigen β-Faktor wieder aus der Betriebserfahrung zu bestimmen. Gezählt werden dürften dann jeweils nur die CMA, bei denen mehr als eine vorgegebene Anzahl von Komponenten ausgefallen ist. Der Nachteil dieser Methode ist, daß für eine größere Anzahl gleichzeitig vorliegender Komponentenausfälle nur sehr begrenzte Betriebserfahrung vorliegt, so daß häufig auf eine Null-Ausfall-Statistik zurückgegriffen werden müßte. Eine realistische Bewertung ist dann oft nicht möglich, d.h., es werden damit in vielen Fällen zu pessimistische Ergebnisse erzielt.

Bei Anwendung des spezialisierten Marshall-Olkin-Modells ("binomial failure rate"-Modell) /5-19/, /5-20/ kann aus der Betriebserfahrung nicht nur eine Ausfallrate oder -wahrscheinlichkeit für CMA, sondern auch ein Parameter, der den Kopplungsgrad zwischen den redundanten Komponenten bzw. Teilsystemen bewertet, ermittelt werden. Somit ist aus vorliegenden Betriebserfahrungen, bei denen eine bestimmte Anzahl von Komponenten betroffen ist, eine Extrapolation auf andere betroffene Komponenten möglich. Allerdings muß auch hier eine durch die Betriebserfahrung ausreichend abgesicherte Datenbasis für die beiden Parameter dieses Modells vorliegen. Werte für die Parameter wurden allerdings bisher für Komponenten von Chemieanlagen nicht bestimmt.

Zusammenfassend ist festzustellen, daß mit dem spezialisierten Marshall-Olkin-Modell ein geeignetes theoretisches Instrument zur Behandlung des überwiegenden Anteiles der bekannten Common-Mode-Ausfälle vorliegt. Für seine erfolgreiche praktische Anwendung ist jedoch entsprechende Betriebserfahrung notwendig. Allerdings ist Voraussetzung, daß die beobachteten CMA durch eine Binomialverteilung beschrieben werden können.

5.5 Menschliches Fehlverhalten beim Betrieb technischer Anlagen

5.5.1 Vorbemerkung

Analyse und Bewertung menschlichen Fehlverhaltens in Mensch-Maschine-Systemen haben mit zunehmender Größe und Komplexität technischer Anlagen und dem häufig damit verbundenen Gefährdungspotential eine wachsende Bedeutung erlangt. Wenn auch die Wahrscheinlichkeit schwerer Störfälle im allgemeinen klein ist, muß doch oft wegen der möglichen großen Konsequenzen solcher Ereignisse alle Anstrengung darauf gerichtet sein, das Risiko der technischen Anlagen zu mindern.

Zahlreiche Studien an komplexen Mensch-Maschine-Systemen sowie die Analyse von Unfällen in verschiedenen technischen Bereichen haben gezeigt, daß die Systemkomponente Mensch häufig einen sehr wesentlichen Beitrag zu tatsächlichen oder potentiellen Systemausfällen liefert. Konsequenterweise wurden damit die Bemühungen immer stärker, Methoden zur Analyse und Bewertung menschlicher Fehlhandlungen zu entwickeln.

Die Analyse und Bewertung menschlicher Fehlhandlungen wird in Risikostudien oder Zuverlässigkeitsanalysen als integraler Bestandteil der Systemanalyse durchgeführt. Daher wird der Mensch als Systemkomponente betrachtet, die eine definierte Aufgabenstellung innerhalb einer vorgegebenen Zeit und innerhalb fester Toleranzgrenzen zu erfüllen hat. Gegenüber sonstigen Systemkomponenten ist der Mensch durch eine wesentlich größere Variabilität und Komplexität gekennzeichnet, die eine Beschreibung erheblich erschwert. Insbesondere komplexe Handlungsabläufe oder Entscheidungssituationen sind einer probabilistischen Behandlung nur schwer zugänglich.

In der Systemanalyse technischer Systeme werden Wahrscheinlichkeitsaussagen zu den Systemkomponenten durch geeignete Zuverlässigkeitskenngrößen getroffen (Abschnitt 5.1). In der Analyse von Mensch-Maschine-Systemen besteht nun die Notwendigkeit, auch die Zuverlässigkeit der Systemkomponente Mensch durch geeignete Zuverlässigkeitskenngrößen zu beschreiben.

Die Klassifizierung menschlicher Fehler kann in vielfältiger Form erfolgen. Eine allgemeinverbindliche Festlegung gibt es dabei nicht. Im folgenden werden die in /5-21/ angegebenen Klassifizierungen verwendet. Danach lassen sich generell zwei Kategorien menschlichen Fehlverhaltens unterscheiden: Fehlverhalten, das durch die Arbeitssituation bedingt ist, und Fehlverhalten, das in der jeweiligen Persönlichkeit (z.B. physische Konstitution) angelegt oder durch Faktoren bedingt ist, die durch persönliche Entscheidungen beeinflußt sind (z.B. Alkoholisierung).

In der Systemanalyse interessiert in der Regel nur das Fehlverhalten, das durch die Arbeitssituation bestimmt ist. Hierbei läßt sich eine weitere Klassifizierung finden, die den durch die Art menschlicher Informationsverarbeitung /5-22/ gegebenen Fehlermöglichkeiten entspricht:

- Unterlassungsfehler:
  Unterlassen oder Auslassen einer Handlung oder eines Arbeitsschrittes
- Handlungsfehler:
  Fehlerhafte Durchführung einer Handlung oder eines Arbeitsschrittes
- Fehler in der Beachtung der Reihenfolge:
  Durchführung einer Handlung oder eines Arbeitsschrittes außerhalb der erforderlichen Reihenfolge
- Zeitfehler:
  Durchführung einer Handlung oder eines Arbeitsschrittes außerhalb der festgelegten Zeit
- Fehler, die vorgesehene Handlung auszuführen:
  Durchführung einer Handlung bzw. eines Arbeitsschrittes, die nicht zum geplanten Ablauf gehören und nicht hätten vorgenommen werden dürfen.

5.5.2 Analytische Behandlung des menschlichen Fehlverhaltens

Grundlegend für die Bewertung menschlichen Fehlverhaltens in der Systemanalyse ist, die für den untersuchten Ereignisablauf wesentlichen Handlungen des Personals zu identifizieren und zu analysieren. Die Vorgehensweise entspricht dabei weitgehend den in der Ergonomie üblichen Aufgabenanalysen. Mit den Mitteln der Systemanalyse werden zunächst alle im betrachteten Ereignisablauf wesentlichen Handlungen nach dem Zeitpunkt ihrer Anforderung und der für ihre Ausführung zur Verfügung stehenden Zeit erfaßt. Darüber hinaus werden die Aufgabenstellung für diese Handlung, die zu ihrer Durchführung benötigten bzw. vorhandenen Informationen und Korrekturmöglichkeiten bei un-

terlassener oder fehlerhafter Ausführung analysiert. Weiterhin werden sonstige, für die menschliche Zuverlässigkeit bedeutsame Einflußgrößen, wie z.B. Kenntnisstand über den jeweiligen Prozeß, ergonomisch günstige oder nachteilige Gestaltung des Arbeitsplatzes, der Arbeitsmittel und der Arbeitsumwelt, erfaßt. Anhand dieser Aufgabenanalyse werden dann quantitative Zuverlässigkeitskenngrößen (in der Regel Ausfallwahrscheinlichkeiten pro Anforderung) den darin auftretenden Handlungen aus vorhandenen Datensammlungen zugeordnet. Liegen für komplexe Handlungsabläufe keine Daten vor, müssen sie so weit in Einzelschritte aufgegliedert werden, bis für diese Einzelhandlungen ausreichendes Datenmaterial vorliegt. Im Rahmen der Fehlerbaumerstellung werden die identifizierten und analysierten menschlichen Fehlhandlungen den betreffenden Systemen und Komponenten zugeordnet.

Wichtig für die Bewertung ist es, mögliche Abhängigkeiten menschlicher Handlungen zu berücksichtigen. Diese Abhängigkeiten können sowohl zwischen Handlungen mehrerer Personen als auch bei aufeinanderfolgenden Handlungen derselben Person (z.B. durch hohen Streß) gegeben sein. Zur Analyse und Bewertung menschlicher Fehlhandlungen wird heute das am meisten verbreitete THERP-Verfahren (Technique for Human Error Rate Prediction) angewendet. Dieses Verfahren ist zusammen mit einer ausführlichen Datenzusammenstellung in /5-21/ dokumentiert. An ihm orientiert sich auch die hier durchgeführte Untersuchung (Abschnitt 6.3.3).

5.5.3 Wichtige Einflußgrößen auf die menschliche Zuverlässigkeit

Im folgenden werden einige wichtige Einflußgrößen auf die menschliche Zuverlässigkeit kurz dargestellt und vor allem Hinweise auf wesentliche Gesichtspunkte in der Analyse und Bewertung der menschlichen Zuverlässigkeit gegeben.

- Ergonomische Gestaltung der Warte

Erhöhte Fehlerwahrscheinlichkeiten sind in den Fällen anzunehmen, bei denen die Anordnung, Kennzeichnung oder das Design der zu bedienenden Steuerungseinrichtungen bzw. der abzulesenden Melde- und Anzeigeeinrichtungen einen Irrtum begünstigen. Zu unterstellen sind solche Einflüsse zum Beispiel, wenn Stereotypen verletzt werden, wenn die Kennzeichnung leicht verwechselt werden kann oder wenn Anzeigen oder Meldungen schlecht ablesbar und ungeeignet sind. Unter Stereotyp wird hier die zu erwartende Reaktion eines Menschen auf einen äußeren Reiz verstanden. So ist zum Beipiel ein grünes Licht (wie bei einer Verkehrsampel) mit der Erwartung von Sicherheit, Gefahrlosigkeit usw. verbunden. Bei Elektrogeräten wird bei Drehung des Reglerknopfes nach rechts ein "mehr", "stärker", "lauter" erwartet (Bewegungsstereotyp).

- Rückkopplung durch Anzeigen und Meldungen

Die Wahrscheinlichkeit menschlicher Fehlhandlungen wird verringert, wenn Rückkopplungen durch Anzeigen und Meldungen gegeben sind, die die Entdeckung und Beherrschung eines begangenen Fehlers wahrscheinlich machen. Eine Fehlerentdeckung ist insbesondere dann zu berücksichtigen, wenn der Operateur unmittelbar nach einer Fehlhandlung durch eine Meldung gewarnt wird, so daß der Fehler bemerkt und korrigiert werden kann. Für die Fehlhandlungen, die eine langsame Änderung von Prozeßgrößen zur Folge haben, ist die Wahrscheinlichkeit, den Fehler zu entdecken, entsprechend geringer.

- Personelle Redundanz

Eine weitere Möglichkeit für die Fehlerentdeckung ist durch personelle Redundanz gegeben. Unter personeller Redundanz wird verstanden, daß an der Entscheidung und/oder an der Durchführung einer Maßnahme mehrere Personen mit ausreichender Quali-

fikation beteiligt sind. Dabei kann sich die Tätigkeit der redundanten Person(en) auf die Kontrolle vorher durchgeführter Maßnahmen beschränken.

- Psychischer Streß

Bei der Bewertung menschlichen Fehlverhaltens ist zu berücksichtigen, ob das Betriebspersonal einer hohen Streßbelastung unterliegt. Bild 5.3 gibt den hypothetischen Zusammenhang zwischen Streßbelastung und menschlicher Zuverlässigkeit wieder. Eine optimale Zuverlässigkeit wird demnach bei einer mäßigen Streßbelastung erreicht, die aber so hoch ist, daß die Aufmerksamkeit des Operateurs voll in Anspruch genommen wird.

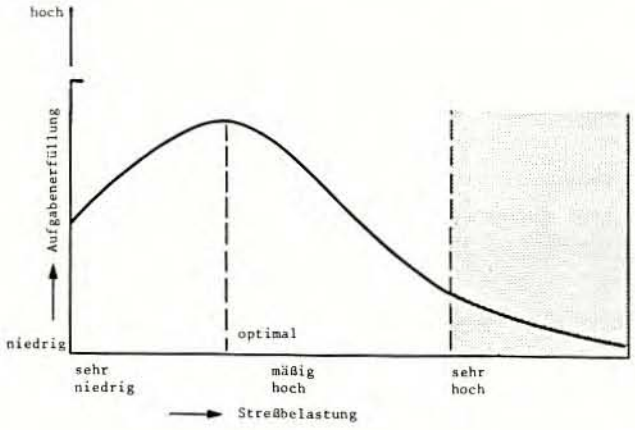


Bild 5.3:
Hypothetischer Zusammenhang zwischen Aufgabenerfüllung und dem bestehenden Streßniveau (aus /5-21/)

Niedrigere Streßbelastungen verschlechtern die Zuverlässigkeit, da uninteressante und wenig fordernde Aufgaben ein Nachlassen der Aufmerksamkeit zur Folge haben. Eine sehr niedrige Streßbelastung liegt z.B. bei routinemäßigen Kontrollgängen vor.

Eine optimale Streßbelastung wird bei Routinetätigkeiten in der Warte während des bestimmungsgemäßen Betriebs der Anlage, bei Wartung, Instandsetzung und Funktionsprüfung zugrunde gelegt. Diese Tätigkeiten führen weder zu übergroßer Anpassung noch sind sie zu anspruchslos. Deshalb kann man davon ausgehen, daß sie zuverlässig durchgeführt werden.

Sehr hoher Streß und damit eine hohe Wahrscheinlichkeit für menschliche Fehlhandlungen liegt kurz nach Auftreten eines Störfalls vor. Abhängig von der Zeit nach Eintritt des Störfalls sind zunehmend niedrigere Wahrscheinlichkeiten für eine menschliche Fehlhandlung anzusetzen. Dabei wird unterstellt, daß die Anlage durch geeignete automatische und menschliche Eingriffe während des Störfallablaufs unter Kontrolle gebracht wird, d.h. sich die Anlagensituation mit zunehmender Zeit bessert und somit die Streßbelastung langsam abklingt.

- Qualifikation und Ausbildung des Personals

Beim Bedienungspersonal komplexer technischer Anlagen kann in der Regel eine sorgfältige Personalauswahl und damit eine ausreichende Qualifikation des Personals vorausgesetzt werden.

Dies gilt nicht in gleichem Maße für das Training des Personals. Hier ist zu unterscheiden zwischen dem Training des Personals vor dem Einsatz in der Anlage, also der aufgabenspezifischen Ausbildung, und dem regelmäßig wiederkehrenden Training, das der Aufrechterhaltung der Fertigkeiten und des Wissens dient. Während in der Regel eine mehr oder minder effektive Ausbildung vor dem Einsatz des Personals durchgeführt wird, ist ein regelmäßig wiederkehrendes Training des Personals oft nicht vorgesehen. Gerade letzteres ist aber für die Aufrechterhaltung des Wissens, insbesondere für Störungssituationen, von sehr großer Bedeutung. Bild 5.4 gibt den hypothetischen Zusammenhang zwischen Training und Aufrechterhaltung der Fähigkeit, mit Notfallsituationen fertig zu werden, wieder.

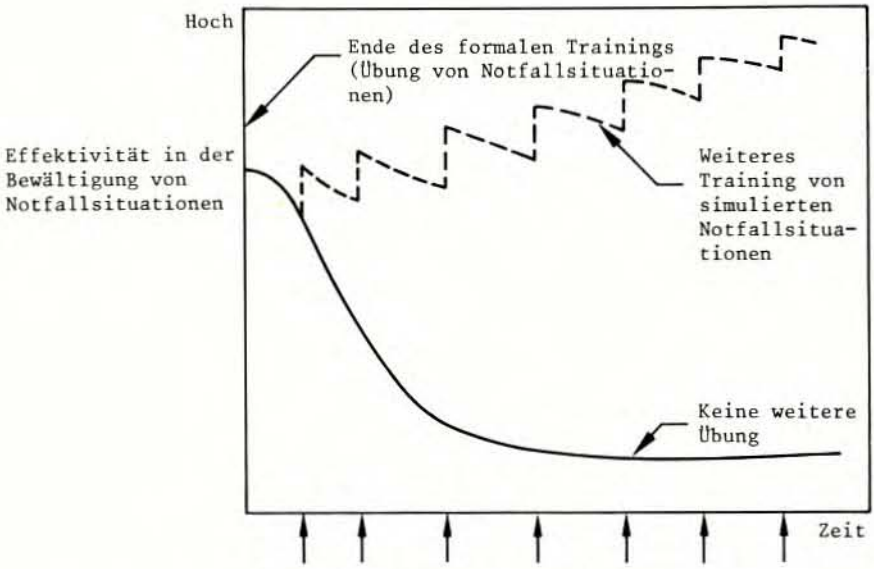


Bild 5.4:
Hypothetischer Zusammenhang zwischen Training und Aufrechterhaltung von Fähigkeiten, Notfallsituationen zu meistern (aus /5-21/)

Hinzu kommt, daß vielfach die Effektivität der Trainingsprogramme nicht überprüft wird. Die Qualität und Regelmäßigkeit des Trainings muß daher in die Analyse und Bewertung der Zuverlässigkeit des Bedienungspersonals einbezogen werden.

- Schriftliche Anweisungen

Im allgemeinen werden geringere Fehlerwahrscheinlichkeiten für Handlungen angesetzt, für die schriftliche Anweisungen vorhanden sind. Um die Qualität schriftlicher Anweisungen zu bewerten, sind Kriterien, wie gute Lesbarkeit und Übersichtlichkeit, bei Störfallanweisungen außerdem übersichtliche und

leicht zugängliche Aufbewahrung, Aktualisierung und Klarheit der Anweisung zu berücksichtigen.

- Abhängigkeit menschlicher Handlungen

Ein wichtiger Einfluß bei der Bewertung menschlicher Zuverlässigkeit ist die Abhängigkeit menschlicher Handlungen untereinander. Es lassen sich zwei Arten von Abhängigkeiten, nämlich direkte und indirekte, feststellen.

Direkte Abhängigkeit menschlicher Handlungen liegt dann vor, wenn eine Abhängigkeit unter den Handlungen selbst besteht. Ein Beispiel dafür sind ähnliche Aufgaben, die von demselben Operateur nacheinander durchgeführt werden (Bedienung von zwei unmittelbar aufeinanderfolgend zu betätigenden Komponenten).

Indirekte Abhängigkeit liegt vor, wenn eine Abhängigkeit zwischen mehreren Handlungen und einem Faktor gegeben ist, der diese gemeinsam beeinflußt. Ein solcher Faktor wäre z.B. ein falsch eingestelltes oder falsch geeichtes Meßgerät, mit dem die Kalibrierung von Meßkanälen erfolgt.

Völlige Unabhängigkeit der Handlungen ist zu erwarten, wenn sie gänzlich unterschiedlich sind oder räumlich und zeitlich voneinander getrennt durchgeführt werden.

6. PROBABILISTISCHE UNTERSUCHUNG EINER ANLAGE ZUR HERSTELLUNG VON HEXOGEN

6.1 Beschreibung der Anlage

6.1.1 Allgemeines

Gegenstand der probabilistischen Untersuchung sind die Verfahrensschritte Nitrieren und Auskochen bei der Herstellung des Sprengstoffs Hexogen (Nr. 142 Anhang II der Störfall-Verordnung). Diese sind Teil eines Gesamtprozesses, der unter dem Namen SH-Verfahren /6-1/, /6-2/, /6-3/ bekannt ist. Sein Ablauf wird schematisch in Bild 6.1 gezeigt.

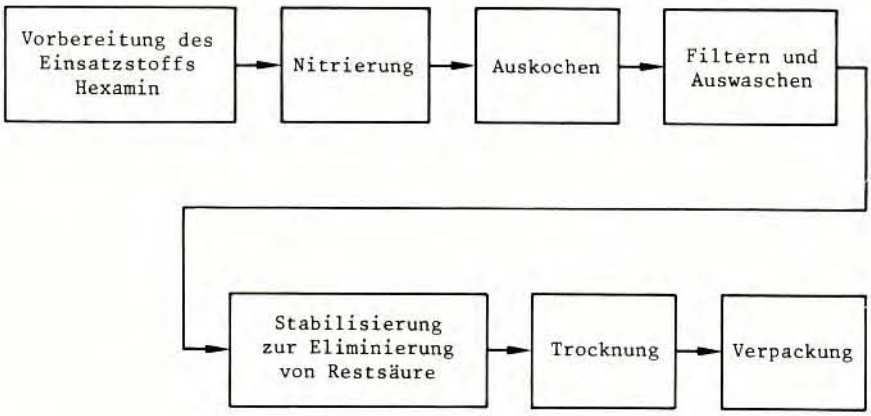


Bild 6.1:
Verfahrensschritte bei der Herstellung von Hexogen

Über die in Bild 6.1 aufgeführten Schritte hinaus sind eine Reihe von Transportvorgängen durchzuführen, die den Materialfluß zwischen den zum Teil in verschiedenen Gebäuden untergebrachten Anlagenteilen sicherstellen. Aus ihnen wurde der hydraulische Transport des Hexogens nach Waschen und Filtern zu

den Druckkochern für die Stabilisierung ausgewählt und ebenfalls probabilistisch untersucht.

Es wird nur der kontinuierliche Betrieb betrachtet. Das wöchentliche An- und Abfahren der Anlage wird nicht analysiert. Einwirkungen von außen wie Flugzeugabsturz, Erdbeben und Folgeschäden aufgrund von Ereignissen in benachbarten Anlagen werden nicht berücksichtigt. Zielsetzung der Untersuchung ist bei Nitrierer und Kocher die Quantifizierung ihrer Sicherheit, während im Falle des hydraulischen Transportsystems die Ausfallhäufigkeit ermittelt wird.

6.1.2 Theoretischer Ablauf des Prozesses und Eigenschaften der hierbei auftretenden Stoffe

Hexogen wird dadurch hergestellt, daß Hexamethylentetramin (Hexamin) mit hochkonzentrierter Salpetersäure (> 98,5 %) reagiert. Dabei erfolgen gleichzeitig mehrere Reaktionen, die sich durch folgende Gleichungen beschreiben lassen /6-1/:

$$(CH_2)_6N_4 + 4HNO_3 \rightarrow (CH_2NNO_2)_3 + 3CH_2O + NH_4NO_3 \qquad (6.1)$$

$$(CH_2)_6N_4 + 6HNO_3 \rightarrow (CH_2NNO_2)_3 + 6H_2O + 3CO_2 + 2N_2 \qquad (6.2)$$

Der Nitrierungsprozeß ist exotherm, wobei in /6-1/ zwei Angaben, nämlich 1158 kJ/kg und 2090 kJ/kg, für die freiwerdende Wärmemenge gemacht werden. Die praktische Durchführung des Prozesses erfordert die vier- bis achtfache Menge des theoretischen Wertes an Salpetersäure. Die Reaktionstemperatur sollte 20 °C nicht übersteigen.

Bei der Reaktion gehen etwa 40 % des im Hexamin enthaltenen Formaldehyds in Hexogen über, während der Rest in Nebenreaktionen verloren geht. Dazu gehören die Hydrolyse von Hexamin, bei der sich Ammoniak und Formaldehyd bilden,

$$(CH_2)_6N_4 + 6H_2O \rightarrow 4NH_3 + 6CH_2O \qquad (6.3)$$

und die Oxidation von Formaldehyd mit Salpetersäure /6-1/

$$2CH_2O + 2HNO_3 \rightarrow 2\ HCOOH + H_2O + NO + NO_2 \qquad (6.4)$$

Darüber hinaus gibt es eine Reihe weiterer Reaktionen, die zu anderen Explosivstoffen als Hexogen führen; sie werden in /6-1/ eingehend beschrieben.

Die Nebenprodukte bewirken, daß das Nitriergemisch chemisch sehr labil ist. Es ist nur so lange haltbar, wie noch Amine anwesend sind, da das gemäß Gleichung (6.4) auftretende NO_2 von den Aminen abgefangen wird. Tritt freies NO_2 auf, so findet eine stürmische Zersetzung des Gemisches statt, die unter besonderen Umständen zur Explosion der gesamten Mischung führen kann. Diese Schwierigkeit wird beim vorliegenden Verfahren dadurch beseitigt, daß das Nitriergut im sogenannten Auskochprozeß stabilisiert wird /6-2/.

Beim Auskochen, das in einem getrennten Reaktor bei ungefähr 75 °C stattfindet, wird das Nitriergut stabilisiert, indem Nebenprodukte durch die Salpetersäure oxidiert werden. Dabei entstehen hauptsächlich die Gase NO_2, NO, N_2 und CO_2.

Es ist offensichtlich, daß an dem beschriebenen Prozeß eine Reihe gefährlicher Stoffe beteiligt sind. Die Eigenschaften der hauptsächlichen Reaktionspartner werden in den Tabellen 6.1 - 6.3 aufgeführt.

Bezüglich der Nebenprodukte ist anzumerken, daß Stickstoffdioxid (NO_2) hochgiftig und korrosiv ist und exotherm mit Wasser reagiert. Formaldehyd (CH_2O) ist bei höheren Temperaturen explosionsfähig /6-4/.

Tab. 6.1:
Eigenschaften von Hexamin ($(CH_2)_6N_4$) /6-4/

Molekulargewicht:	140,19
Schmelzpunkt:	280 °C
Dichte bei -5 °C:	1,331 $\frac{g}{cm^3}$
Toxikologie:	Kontakt mit dem Stoff oder seinen Dämpfen kann bei manchen Personen Hautausschlag hervorrufen;
Feuergefährlichkeit:	moderat unter Hitzeeinwirkung oder bei Kontakt mit Feuer; kann mit oxidierenden Stoffen reagieren.

Tab. 6.2:
Eigenschaften von Salpetersäure (HNO_3) /6-4/

Molekulargewicht:	63,02
Schmelzpunkt:	-42 °C
Siedepunkt:	86 °C
Dichte:	1,5 $\frac{g}{cm^3}$
Toxikologie:	greift Schleimhäute an;
Feuergefährlichkeit:	gering, kann bei Kontakt mit stark reduzierenden Stoffen explodieren;
Unglücksgefahr:	gefährlich; kann hochgiftige NO_x-Gase und Salpetersäuredämpfe abgeben, wenn sie bis zur Zersetzung aufgeheizt wird; reagiert mit Wasser und Dampf unter Abgabe von Wärme sowie giftigen und korrosiven Dämpfen.

Tab. 6.3:
Eigenschaften von Hexogen ($C_3H_6N_6O_6$) /6-4/, /6-5/

Molekulargewicht	222,15
Schmelzpunkt:	202 °C
Bildungsenergie: (bei konstantem Druck)	318,3 $\frac{kJ}{kg}$
Sauerstoffwert:	-21,6 %
Stickstoffgehalt:	37,84 % N
Explosionswärme:	6025 $\frac{kJ}{kg}$
Dichte:	1,82 $\frac{g}{cm^3}$
Bleiblockausbauchung:	480 ml (BAM)
Detonationsgeschwindigkeit:	8750 $\frac{m}{s}$ bei Maximaldichte
Verpuffungspunkt:	230 °C
Schlagempfindlichkeit:	7,4 J
Reibempfindlichkeit:	12 kg Stiftbelastung
Grenzdurchmesser Stahlhülsentest:	8 mm
Toxikologie:	epileptische Anfälle bei Kontakt mit Hexogen sind bekanntgeworden
Feuergefährlichkeit:	mäßig, durch spontane chemische Reaktion
Explosionsgefahr:	einer der stärksten derzeit verwendeten Sprengstoffe; hat höhere Brisanz als TNT
Unglücksgefahr:	gefährlich, stark oxidierend, bei Zersetzung Abgabe giftiger Dämpfe

6.1.3 Technische Prozeßdurchführung

Die im vorangehenden Abschnitt beschriebenen Reaktionen laufen im Nitrierer und Kocher der Hexogenanlage kontinuierlich ab. Beide Einrichtungen sind zusammen mit ihren Hilfsanlagen im Bild 6.2 dargestellt.

Die Reaktionen verlaufen bei Atmosphärendruck. In den Kühlkreisläufen wird lediglich ein Druck aufgebaut, um die Reibungswiderstände zu überwinden. Das System ist mithin praktisch drucklos.

6.1.3.1 Nitrierer

Hochkonzentrierte Salpetersäure wird dem Industriekomplex in Tankwagen angeliefert und in einen Lagertank gefüllt, aus dem der Tagestank "1" gespeist wird. Von diesem Tank aus wird die Säure von einer der beiden redundanten Pumpen (41GA-01A oder 41GA-01B) in den Vorlagebehälter "2" gefördert. Dieser ist mit einem Überlauf versehen, durch den zu viel geförderte Säure in den tiefer gelegenen Tagestank "1" zurückläuft. Auf diese Weise wird im Normalbetrieb ein konstanter Salpetersäurespiegel im Vorlagebehälter aufrechterhalten. Die Säure wird dort auf ca. 4 °C abgekühlt. Dies erfolgt durch Kühlschlangen, die Teil des im Abschnitt 6.1.4.1 beschriebenen Kühlkreislaufes sind. Aus dem Vorlagebehälter fließt die Salpetersäure in den tiefer gelegenen Nitrierreaktor "3". Der notwendige Durchfluß wird zu Beginn des wöchentlichen Produktionszyklus von Hand am Ventil "4" eingestellt.

Hexamin von geeignetem Feuchtegehalt und geeigneter Korngröße wird mit einem Kübelförderer diskontinuierlich in den Bunker "5" geliefert. Das Hexamin fällt aus dem Bunker, der zur Verbesserung des Fließens mit einem Rüttler ausgerüstet ist, auf die Förderschnecke "6" und von dort in den tiefer gelegenen Nitrierer "3". Der notwendige Durchsatz wird durch Einstellung einer entsprechenden Drehzahl des Förderschneckenantriebs "7" zu Beginn des Produktionszyklus sichergestellt.

Im Nitrierer laufen die in Abschnitt 6.2 beschriebenen exothermen Reaktionen ab. Damit die Reaktionstemperatur 20 °C nicht übersteigt, wird der Reaktor gekühlt. Dazu dienen die nicht regelbare Kühlung des Mantels und die regelbare Kühlung mit Kühlschlangen im Inneren des Reaktors. Beide sind Teile des Kühlkreislaufes, der in Abschnitt 6.1.4.1 beschrieben wird. Um eine möglichst gleichmäßige Durchmischung sämtlicher an der Reaktion beteiligter Stoffe zu gewährleisten und lokales Überschreiten der maximal zulässigen Reaktionstemperatur zu vermeiden, ist der Reaktor mit dem Rührer "8" ausgerüstet. Er wird von einem Ölhydraulikmotor angetrieben, dessen Drehzahl in weiten Bereichen regelbar ist.

Durch einen Überlauf verläßt die Stoffmischung den Nitrierer und strömt in einen ähnlich aufgebauten tiefer gelegenen Nachnitrierer, der im Bild 6.2 nicht gezeigt wird. Dort wird die Reaktion fortgesetzt, ohne daß die Ausgangsstoffe erneut zugeführt werden.

Die Gase, die bei Nitrierung und Nachnitrierung entstehen (Abschnitt 6.2), werden gesammelt und von einem Gebläsesystem, das aus zwei redundant angeordneten Ventilatoren besteht, über Dach abgeführt.

Im Anschluß an die Nachnitrierung strömt die Mischung aus Hexamin, Hexogen, Salpetersäure und Nebenprodukten in den wiederum tiefer gelegenen Kocher "9", der im nächsten Abschnitt dargestellt wird.

6.1.3.2 Kocher

Der Gefahr einer Zersetzung des im Nitrierer befindlichen Gemisches, die durch ungebundenes NO_2 hervorgerufen werden kann, wird dadurch begegnet, daß der Nitrierung ein Auskochprozeß im Kocher "9" nachgeschaltet wird. Dort werden die im Nitriergut enthaltenen Nebenprodukte bei einer Temperatur von ca. 75 °C durch die Salpetersäure oxidiert. Das Hexogen, welches das

Auskochen ohne Verlust übersteht, liegt nach dem Prozeß als Suspension in einer 55%igen Salpetersäure vor.

Da der Prozeß stark exotherm ist, verfügt der Kocher "9" über eine nicht regelbare Mantelkühlung und ein regelbares System von Kühlschlangen, die in seinem Inneren verlaufen. Beide sind Teile des Wasserkühlkreislaufes, der im Abschnitt 6.1.4.2 näher beschrieben wird. Für eine gute Durchmischung und eine möglichst gleichmäßige Temperaturverteilung im Kocher sorgt der Rührer "10", der von einem Ölhydraulikmotor angetrieben wird und dessen Drehzahl in weiten Bereichen regelbar ist. Der Auskochprozeß wird in zwei nachgeschalteten Kochern, die im Bild 6.2 nicht gezeigt werden, fortgeführt. Dabei wird die Temperatur der Stoffe stufenweise auf 25 °C abgesenkt.

Die Kocher sind mit einer Anlage zum Absaugen der bei der Oxidation entstehenden Gase, hauptsächlich NO_2, NO, N_2 und CO_2, ausgerüstet. Diese besteht aus dem Abscheider "11" und den zwei redundant angeordneten Gebläsen 41GD-02A und 41GD-02B. Die Gase werden normalerweise einer Absorptionseinheit zugeführt, können aber im Notfall mit Hilfe des Ventils "12" über Dach abgeblasen werden. Nach dem Auskochprozeß wird die Mischung gefiltert, um das Hexogen von den restlichen Mischungsbestandteilen abzutrennen.

6.1.4 Hilfseinrichtungen

Wie bereits erwähnt, sind sowohl das Nitrieren als auch das Auskochen stark exotherme Vorgänge. In beiden Fällen gelten gewisse obere Grenzen für die Prozeßtemperatur (20 °C bzw. 80 °C). Um diese Grenzen einzuhalten, sind Kühlsysteme vorgesehen. Die Kühlung des Nitrierers arbeitet wegen der relativ geringen Temperaturen mit einer Mischung von 25 % Methanol in Wasser, wobei das Methanol als Einfrierschutz dient. Die Kocher verfügen über ein eigenes Kühlsystem, in dem Wasser als Kühlmittel verwendet wird. Beide Kühlsysteme werden nachfolgend beschrieben.

6.1.4.1 Nitriererkühlung

Der Kühlkreislauf besteht aus zwei Kühlschleifen, dem Kühlmittelbehälter "13", zwei redundant ausgelegten Pumpstationen und dem Verdampfer "14", der mit einem Kühlaggregat üblicher Bauart verbunden ist. In der einen Schleife wird das Kühlmittel, dessen Temperatur ca. -5 °C beträgt, von einer der beiden Pumpen 40GA-02A oder 40GA-02B aus der kalten Seite des Kühlmittelbehälters angesaugt und nach erfolgter Kühlung in dessen warme Seite zurückgefördert. Gekühlt werden:

- der Salpetersäurevorlagebehälter "2",
- der Mantel des Nitrierers "3",
- die Kühlschlangen im Nitrierer "3".

Während der Salpetersäurevorlagebehälter und der Mantel des Nitrierers ungeregelt gekühlt werden, wird der Massenstrom, der die Kühlschlangen im Inneren des Nitrierers "3" durchläuft, geregelt. Dazu wird die Temperatur im Reaktor vom Meßwertgeber TE 07A gemessen, im I/P-Wandler TY 07A in ein Druckluftsignal umgewandelt und dem Regler TIC 07A als Istwert zugeführt. Dieser Regler hält über die Regelarmatur TV 07A die Reaktionstemperatur konstant.

In der zweiten Schleife wird das Kühlmittel nach der Wärmeaufnahme im Vorlagebehälter und Nitrierer rückgekühlt. Zu diesem Zweck wird es von einer der redundanten Pumpen 40GA-01A oder 40GA-01B aus der warmen Seite des Kühlmittelbehälters "13" angesaugt und nach Wärmeaustausch im Verdampfer "14" der kalten Seite des Kühlmittelbehälters zugeführt.

Im Verdampfer "14" wird die Temperatur des Kühlmittels von 1 °C auf -5 °C abgesenkt. Die Wärme wird ihm dabei durch Verdampfen von Frigen im Kühlaggregat, dessen Einzelheiten in Bild 6.2 nicht gezeigt werden, entzogen.

Die Regelung des Kühlaggregates erfolgt über den Temperaturschalter TS 4001, der die Temperatur des Kühlmittels, das

in die kalte Seite des Kühlmittelbehälters zurückläuft, überwacht.

6.1.4.2 Kocherkühlung

Die Kocher werden durch einen offenen Wasserkühlkreislauf gekühlt. Das kalte Kühlwasser wird aus der Bodentasse des Naßkühlturms "15" von einer der beiden redundanten Pumpen 40GA-04A oder 40GA-04B angesaugt und durch die Mantelkühlrohre und die Kühlschlangen im Inneren des Kochers gepumpt, wo es die Wärme, die beim Auskochen entsteht, aufnimmt. Anschließend wird es zum Wasserverteiler des Kühlturms "15" gefördert, aus dem es fein verteilt abregnet. Die dabei auftretende Verdampfung kann durch den vom Motor 40 GDM 01 angetriebenen Ventilator gefördert werden. Dieser wird in Abhängigkeit von der Temperatur des abgekühlten Wassers vom Temperaturschalter TSL 07 ein- bzw. ausgeschaltet. Das bei der Kühlung verdunstende Wasser wird ersetzt.

Zu diesem Zweck ist das Schwimmerventil LCV 02 vorgesehen, das bei niedrigem Niveau in der Bodentasse die Wasserzufuhr öffnet. Um ein Einfrieren des Kühlwassers bei Außentemperaturen unter 0 °C zu verhindern, ist eine elektrische Widerstandsheizung vorhanden, die vom Temperaturschalter TSLL 08 bei zu geringen Kühlwassertemperaturen eingeschaltet wird.

Während der Massenstrom der Mantelkühlung nicht geregelt wird, läßt sich der Durchfluß durch die Kühlschlangen auf zwei Arten regeln: Zum einen wird mit dem Handregler HC 13 das Handventil HV 13 auf einen bestimmten Durchfluß eingestellt, zum andern wird über den Temperaturmeßwertgeber TE 17 und den I/P-Wandler TY 17 ein pneumatisches Signal auf den Regler TIC 17 gegeben, der seinerseits das pneumatische Ventil TV 17 so verstellt, daß die Kochertemperatur eingehalten wird. Die Kombination von manueller und automatischer Regelung hat den Vorteil, daß die Handarmatur so eingestellt werden kann, daß die pneumatische Armatur in ihrem optimalen Regelbereich arbeitet.

6.1.5 Sicherheitseinrichtungen

6.1.5.1 Allgemeines

Wie in Abschnitt 6.1.2 ausgeführt, weisen die am Prozeß beteiligten Stoffe ein erhebliches Gefahrenpotential auf. Um dieses unter Kontrolle zu halten, ist es notwendig,

- die Nitrierreaktion mit einem Überschuß an Salpetersäure durchzuführen,
- die Nitrierreaktion bei Temperaturen um 10 °C ablaufen zu lassen,
- den Auskochprozeß bei Temperaturen um 75 - 80 °C durchzuführen,
- die Gase aus dem Kocher kontrolliert abzuleiten,
- im Nitrierer und Kocher für eine gute Durchmischung zu sorgen, damit lokale Überschreitungen der Prozeßtemperatur vermieden werden.

Neben den bereits beschriebenen Regelvorrichtungen, die für eine Einhaltung der Prozeßbedingungen sorgen sollen, sind für den Fall ihres Versagens Sicherheitseinrichtungen vorgesehen. Diese umfassen die Möglichkeit,

bei der Nitrierung
- die Hexaminzufuhr abzuschalten und
- den Inhalt des Nitrierers in den Notablaßtank zu entleeren,

beim Auskochen
- den Kocherinhalt in einen Notablaßtank zu entleeren und
- die entstehenden Gase über Dach abzuleiten.

Die für die Sicherheit wichtigen Einrichtungen sind notstromgesichert oder verfügen über eine eigene batteriegepufferte Gleichstromversorgung.

Nachfolgend werden die vorhandenen Einrichtungen im einzelnen beschrieben. Im allgemeinen finden hier nur diejenigen Instrumente Erwähnung, die auf der Warte abgelesen werden können

oder dort einen Alarm auslösen. Darüber hinaus verfügt die Anlage noch über zahlreiche lokale Instrumente, die jedoch nicht im Bild 6.2 gezeigt werden, da die nachfolgende Analyse generell keinen Rückgriff auf sie macht.

6.1.5.2 Sicherheitseinrichtungen des Nitrierers und seiner Kühlung

- Kühlung

Der Durchfluß auf der warmen Seite wird mit Hilfe des Durchflußmessers FAL 01 überwacht, der beim Unterschreiten eines Grenzwertes ein Alarmsignal auf der Warte gibt. Eine Temperaturüberwachung dieses Bereichs erfolgt nicht.

Auf der kalten Seite des Kühlkreislaufs werden Temperatur und Druck überwacht. Über den Temperaturmeßwertgeber TE 04 wird durch das Instrument TI 04 die Temperatur auf der Warte angezeigt und bei Überschreiten eines Grenzwertes durch das Gerät TAH 04 ein Alarmsignal gegeben. Herrscht in der Kühlmittelleitung ein zu geringer Druck, so wird über das Gerät PAL 06 ein Alarm auf der Warte ausgelöst. Darüber hinaus wird durch den Druckschalter PSL 07 die Stromzufuhr zum Antrieb der Hexamindosierschnecke unterbrochen und somit die Hexaminzufuhr zum Nitrierer gestoppt.

- Reaktionstemperatur

Über die Meßkette der Kühlungsregelung TE 07A und TY 07A wird vom pneumatischen Alarmgeber TAH 07A bei zu hohen Reaktionstemperaturen ein Alarm auf der Warte ausgelöst. Der zeitliche Temperaturverlauf wird vom Instrument TR 07A aufgezeichnet.

- Zufuhr der Salpetersäure

Die Stromzufuhr zum Antrieb der Hexaminförderschnecke wird durch folgende Auslösesignale aus dem Bereich der Salpetersäurezufuhr unterbrochen:

- Ausfall der in Betrieb befindlichen Förderpumpe für Salpetersäure 41GA-01A oder 41GA-01B über Motorendkontakt,
- zu niedriges Salpetersäureniveau im Vorlagebehälter "2" über den Niveauschalter LSL 04,
- zu geringer Durchfluß in den Nitrierer über den Durchflußmesser FSL 02A.

In allen Fällen wird die Hexaminzufuhr zum Nitrierer beendet. Darüber hinaus ertönt ein Alarm auf der Warte, der von folgenden Geräten ausgelöst werden kann:

- LAL 04 bei zu niedrigem Niveau im Vorlagebehälter "2",
- FAD 01A bei zu geringem Durchfluß von Salpetersäure zum Nitrierer,
- FAL 02A bei zu geringem Durchfluß von Salpetersäure zum Nitrierer.

Die Durchflußmesser FAD 01A und FAL 02A sind so aufeinander abgestimmt, daß zunächst ein Alarm vom Gerät FAD 01A und bei weiter sinkendem Massenstrom vom Instrument FAL 02A ausgelöst wird. Dann kommt es außerdem zur Abschaltung der Hexaminzufuhr über den Durchflußschalter FSL 02A.

- Überwachung der Rührerdrehzahl

Ein Absinken der Rührerdrehzahl unter den unteren Grenzwert löst über den Drehzahlmesser SAL 04A einen Alarm auf der Warte aus. Übersteigt die Drehzahl einen maximalen Wert, etwa durch Bruch von Rührerschaufeln oder -welle, kommt es über das Instrument SAH 04A zum Alarm.

- Notablassen

Für die Anregung des Notablassens bei zu hoher Reaktionstemperatur ist eine eigene Meßkette vorgesehen, deren Elemente an eine batteriegepufferte Gleichstromversorgung angeschlossen sind. Sie besteht aus dem Temperaturmeßwertgeber TE 08A, dem Temperaturanzeiger TI 08A und den Temperaturschaltern TSH 08A und TSHH 08A.

Über das Gerät TI 08A läßt sich die Reaktionstemperatur auf der Warte ablesen. Übersteigt diese einen ersten Grenzwert, so wird die Hexaminzufuhr zum Nitrierer über den Temperaturschalter TSH 08A unterbrochen. Steigt die Temperatur weiter, aktiviert der Temperaturschalter TSHH 08A den Rührermotor 41 GFM 08A im Notablaßtank und das Magnetventil SV 01A. Durch die Änderung der Ventilstellung wird das Ablaßventil HV 01A vom Druck der Instrumentenluft entlastet, so daß es den Weg für das Nitriergut in den tiefer gelegenen Notablaßtank "16" freigibt. Das Ventil HV 01A ist "fail-safe" ausgelegt; es öffnet bei Versagen der Druckluftversorgung.

Das Notablassen kann über das Temperatursignal und durch Knopfdruck eingeleitet werden. Entsprechende Druckschalter sind sowohl auf der Warte als auch vor Ort vorgesehen. Dabei ist es möglich, jeden Nitrierer und Kocher einzeln sowie auch Gruppen mehrerer Einheiten gemeinsam anzusprechen. Im Notfall läßt sich das Ablaßventil auch von Hand öffnen.

Das Notablassen hat den Verlust des Produktes zur Folge und ist deshalb erst als letzte Sicherheitsmaßnahme vorgesehen.

6.1.5.3 Sicherheitseinrichtungen des Kochers, seines Kühlkreislaufs und seines Gasabzugs

- Wasserkühlung

Bei niedrigem Druck im Wasserkühlkreislauf wird vom Alarmgerät PAL 09 ein Alarmsignal auf der Warte gegeben.

- Überwachung der Kochertemperatur

Über den Meßwertgeber TE 17 und den I/P-Wandler TY 17 der Kühlungsregelung erfolgt eine Anzeige der Kochertemperatur durch das pneumatische Gerät TI 17 auf der Warte. Beim Überschreiten eines oberen Grenzwertes wird vom pneumatischen Instrument TAH 17 ein Alarm ausgelöst. Darüber hinaus wird der zeitliche Temperaturverlauf vom Instrument TR 17 aufgezeichnet.

- Überwachung der Rührerdrehzahl

Die Überwachung der Rührerdrehzahl erfolgt entsprechend den Ausführungen im Abschnitt 6.1.5.2. Bei Unterschreiten des Grenzwertes für die Drehzahl wird vom Gerät SAL 06, beim Überschreiten durch SAH 06 ein Alarm auf der Warte ausgelöst.

- Gasabzug

Die Zusammensetzung der Gase kann aufgrund einer charakteristischen Färbung von der Warte aus mit Hilfe eines Farbfernsehgeräts beurteilt werden, so daß bei Abweichungen von der Norm, die auf einen nicht ordnungsgemäßen Verlauf des Auskochens hindeuten und zu einer Änderung der Farbe der Abgase führen, eine Überprüfung der Prozeßparameter an Hand der Warteninstrumentation durchgeführt werden kann. Gegebenenfalls kann der Kocherinhalt in den Notablaßtank "17" entleert werden.

Im Falle eines Versagens des Betriebsmotors (41GD-02A oder 41GD-02B) wird durch einen Endschalter der jeweilige Reservemotor eingeschaltet. Diese Einrichtung wirkt nur bei Motorstillstand, nicht aber bei Schäden am Ventilflügel oder bei Keilriemenriß. In solchen Fällen und auch bei Verstopfungen in den Leitungen oder im Abscheider erfolgt ein Alarm auf der Warte wegen ansteigenden Drucks über das Instrument PAH 12.

Gleichzeitig öffnet der Druckschalter PSH 12 das Motorventil "12", das einen Abzug der Gase über Dach erlaubt.

- Notablassen

Bei zu hohen Temperaturen im Kocher wird vom Meßwertgeber TSH 18 das Magnetventil SV 03 angesprochen. Dieses entlastet das Notablaßventil HV 03 vom Druck der Instrumentenluft, so daß der Inhalt des Kochers in den tiefer gelegenen Notablaßtank "17" abläuft. Gleichzeitig wird der Rührer des Notablaßtanks 41 GFM 08B in Betrieb genommen. Im übrigen gelten die Ausführungen des Abschnitts 6.1.5.2.

6.1.5.4 Notablaßtanks

Die Notablaßtanks "16" und "17", die den Inhalt des Nitrierers bzw. Kochers beim Notablassen aufnehmen, sind mit Wasser gefüllt. Um zu vermeiden, daß dies bei Außentemperaturen unter 0 °C gefriert und somit die Notablaßtanks nicht funktionsfähig sind, sind die Alarme TAL 31A bzw. TAL 31B vorgesehen, die zu niedrige Temperaturen in den beiden Tanks auf der Warte anzeigen. Die Tanks können dann von außen mit Prozeßdampf gewärmt werden. Sie sind mit Rührern versehen (41 GFM 08A im Tank "16" und 41 GFM 08B im Tank "17"), die beim Notablassen in Betrieb genommen werden.

6.1.5.5 Notstromversorgung

Die Anlage ist mit Notstromdieseln ausgerüstet, die folgende im Rahmen der Analyse wichtige Einrichtungen versorgen:

- Ventilatoren zum Absaugen der Gase aus dem Kocher (41GD-02A/B),
- Druckölversorgung und damit die Rührer im Nitrierer und Kocher,

- Pumpen im kalten Teil des Kühlmittelkreislaufs (40GA-02A/B),
- Pumpen im warmen Teil des Kühlmittelkreislaufs (40GA-01A/B),
- Pumpen des Wasserkühlkreislaufs des Kochers (40GA-04A/B).

Bei Netzausfall kommt die Hexaminzufuhr zum Erliegen. Anschließend ist die Salpetersäurezufuhr zu unterbinden. Spricht die Notstromversorgung an, ist ein Entleeren der Reaktoren in die Notablaßtanks nicht vorgesehen, damit das Produkt nicht verloren geht. Funktioniert die Notstromversorgung jedoch nicht, ist mit einem Ansprechen des Notablassens zu rechnen, dessen Meßkette und Magnetventil unabhängig von Netz und Generator durch Batterien versorgt werden. Sollte das Ablassen nicht automatisch erfolgen, müßte es von Hand ausgelöst werden. Unabhängig vom Funktionieren oder Versagen der Notstromversorgung wird die Anlage im Notstromfall abgefahren.

6.1.6 Hydraulisches Transportsystem

6.1.6.1 System- und Funktionsbeschreibung

Nach dem Filtern wird das Hexogen mit Hilfe des hydraulischen Transportsystems, das in Bild 6.3 dargestellt ist, zur Stabilisierung gefördert. Die Förderanlage arbeitet mit Hilfe eines Diffusors. Das Hexogen wird gleichzeitig mit Wasser in den Trichter "1" eingebracht. Dort entsteht im Sog, den der Diffusor "2" hervorruft, ein fließfähiges Flüssig-Feststoffgemisch. Dieses Flüssig-Feststoffgemisch wird durch die Rohrleitungen zum Dreiwegeventil XV 01A transportiert und dort auf die kippbaren Nutschen "3" der verschiedenen Stabilisierungsreaktoren (Bild 6.3 zeigt nur einen) verteilt. Die Nutschen, die auch Filterwirkung haben, werden nach Erreichen eines vorgegebenen Füllstandes in den Eingangstrichter des Stabilisierungsreaktors "4" entleert.

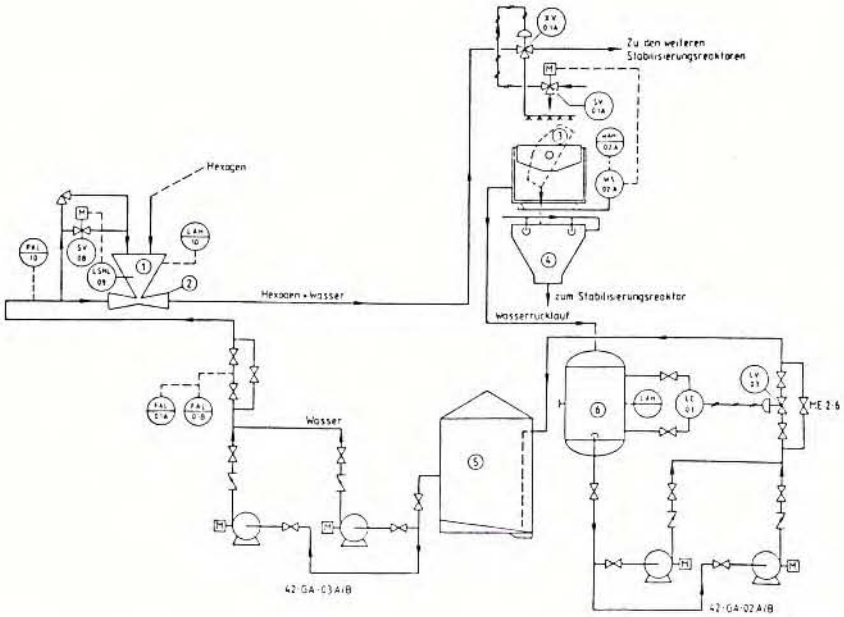


Bild 6.3:
Schematische Darstellung des hydraulischen Transportsystems

Angetrieben wird das Fördersystem von einer der Pumpen 42-GA-03A oder 42-GA-03B, die das Transportwasser, das aus dem Behälter "5" angesaugt wird, durch das Rohrleitungssystem treibt. Vor dem Diffusor wird aus der Rohrleitung Wasser abgezweigt, um den Trichter "1", in dem das Flüssig-Feststoffgemisch entsteht, zu bespeisen. Das Transportwasser, das sich im Kontakt mit dem Hexogen mit Spuren von Salpetersäure anreichert, wird nach Durchlaufen der Nutsche in den Vakuumseparator "6" eingeleitet und gereinigt. Anschließend wird es von einer der beiden Pumpen 42-GA-02A oder 42-GA-02B in den Transportwasserbehälter "5" gefördert, aus dem es erneut in Umlauf gesetzt wird.

6.1.6.2 Sicherheitseinrichtungen

Das System verfügt über die folgenden Sicherheitseinrichtungen:

- Alarm auf der Warte bei hohem Niveau im Trichter "1" über das Instrument LAH 10,
- Alarm auf der Warte bei zu niedrigem Druck vor dem Diffusor über das Instrument PAL 10,
- Alarm bei zu geringem Durchfluß über die Instrumente FAL 01A und FAL 01B auf den Warten für die Nitrierung und die Stabilisierung,
- Abschaltungsmöglichkeit für die Pumpen 42-GA-03A/B von der Warte aus,
- Regelung des Füllstandes im Trichter "1" durch die Regelung eines Teilstroms der Wasserzufuhr über das Ventil SV 08 mit Hilfe des Füllstandreglers LSHL 09.

6.2 Fehlerbaumerstellung

6.2.1 Allgemeines

Die im vorangehenden Kapitel beschriebenen Anlagenteile der Hexogenherstellung wurden mit Hilfe von Fehlerbaumanalysen (Kapitel 4) untersucht. Dabei wurden die folgenden unerwünschten Ereignisse zugrunde gelegt:

- Explosion im Nitrierer,
- Explosion im Kocher,
- Ausfall des hydraulischen Transportsystems.

Gegenüber einem möglichen Auftreten von Explosionen wurden etwaige toxische Belastungen, die sich aus einer Freisetzung von Stoffen aus dem Prozeß ergeben könnten, vernachlässigt. Das jeweilige unerwünschte Ereignis tritt dann auf, wenn nach Eintreten eines störfallauslösenden Ereignisses die zu seiner Beherrschung durch die Anlage notwendigen Betriebs- und Sicherheitssysteme versagen. Die Häufigkeit für das Eintreten

eines unerwünschten Ereignisses aufgrund eines bestimmten auslösenden Ereignisses h_j ergibt sich dann als Produkt aus dessen Eintrittshäufigkeit s_j und der aus der Fehlerbaumauswertung stammenden bedingten Wahrscheinlichkeit für das Versagen der zu seiner Beherrschung erforderlichen Betriebs- und Sicherheitssysteme (Systemfunktion) u_j, d.h.

$$h_j = s_j \cdot u_j \tag{6.5}$$

Die Gesamthäufigkeit für das Auftreten des unerwünschten Ereignisses h errechnet sich als Summe über die Beiträge aus allen auslösenden Ereignissen

$$h = \sum_{j=1}^{J} s_j \cdot u_j \tag{6.6}$$

In Gleichung (6.6) bedeutet J die Anzahl der betrachteten auslösenden Ereignisse. Dabei handelt es sich um das Versagen betrieblicher Komponenten wie Pumpen oder Regelorgane oder den Integritätsverlust von Leitungen. Die Tabellen 6.4 bis 6.6 geben Auskunft über die im Einzelfall zugrundegelegten Ereignisse und deren erwartete Eintrittshäufigkeiten.

Für Nitrierer, Kocher und hydraulisches Transportsystem wurde jeweils ein Gesamtfehlerbaum erstellt, welcher - falls erforderlich - der Übersicht halber in Teilfehlerbäume aufgeteilt wurde. Die Fehlerbäume sind in den Abbildungen 6.4 bis 6.15 dargestellt. Zwischen ihnen bestehen die folgenden Zusammenhänge:

- Explosion im Hauptnitrierer (Fehlerbaum 7, Bild 6.10); zugehörige Teilfehlerbäume:
  - Fehlerbaum 1 (Bild 6.4): Ausfall "warmer Teil" des Kühlmittelkreislaufs

Tab. 6.4:

Auslösende Ereignisse und ihre Eintrittshäufigkeiten für eine Explosion im Nitrierer

Störfallauslösende Ereignisse				Häufigkeit des auslösenden Ereignisses $s_j(a^{-1})$
Ereignis Nr.	Ausgefallene Komponente für das auslösende Ereignis			
	Schlüssel des Fehlerbaumeingangs	Fehlerbaum	Bezeichnung	
N1.1	TY7A41EB01ABVL	3	Umformer	$5,5 \cdot 10^{-1}$
N1.2	TE07A41EB01ABVL	3	Temperaturmessung	$3,1 \cdot 10^{-2}$
N2.1	TV07A41139BV	3	Regelventil	$2,5 \cdot 10^{-1}$
N2.2	TIC07A4139BVL	3	Regler	$3,9 \cdot 10^{-1}$
N3.1	TS.40001BV	1	Thermostatschalter	$3,2 \cdot 10^{-2}$
N3.2	40ED-01BV	1	Rückkühlsystem	1,8
N4	LE40010-40001	1	Leckage	$2,2 \cdot 10^{-2}$
N5	ROHRL.N.DRSCH	2	Leckage	$8,8 \cdot 10^{-4}$
N6	40GA-01ABV	1	warme Pumpe	$3,9 \cdot 10^{-1}$
N7	40GA-02ABV	2	kalte Pumpe	$3,9 \cdot 10^{-1}$
N8	41GA-01ABV	4	HNO_3-Pumpe	1,6
N9	41-EB-01ALE	7	Leckage	$8,8 \cdot 10^{-4}$
N10	41-GF-01ABR	6	Rührer	$1,8 \cdot 10^{-3}$
N11.1	41-GF-01ABV	6	Rührermotor	$8,8 \cdot 10^{-3}$
N11.2	41-GS01BV	6	Hydraulikversorgung	$7,0 \cdot 10^{-2}$

Die Schlüssel beziehen sich auf die Fehlerbäume der Bilder 6.4 bis 6.10.

- Fehlerbaum 2 (Bild 6.5): Ausfall der Solekühlung (gemeinsamer "kalter Teil") und Ausfall der Abschaltung der Hexaminzufuhr bei Kühlungsausfall
- Fehlerbaum 3 (Bild 6.6): Ausfall der Kühlungsregelung Hauptnitrierer
- Fehlerbaum 4 (Bild 6.7): Ausfall der Salpetersäureversorgung
- Fehlerbaum 5 (Bild 6.8): Ausfall Ablassen bzw. Abschalten des Nitrierers
- Fehlerbaum 6 (Bild 6.9): Ausfall "Rührer des Nitrierers"

Tab. 6.5:

Auslösende Ereignisse und ihre Eintrittshäufigkeiten für eine Explosion im Kocher

Störfallauslösende Ereignisse				Häufigkeit des auslösenden Ereignisses $s_j(a^{-1})$
Ereignis Nr.	Ausgefallene Komponente für das auslösende Ereignis			
	Schlüssel des Fehlerbaumeingangs	Fehlerbaum	Bezeichnung	
K1.1	40EG01MOTBV	8	Motor für Kühlturmventilator	$1,8 \cdot 10^{-1}$
K1.2	TSL0740EG01BVC	8	Temperaturschalter für Ventilatorsteuerung	$3,2 \cdot 10^{-2}$
K1.3	TSLL0840EG01BV	8	Temperaturschalter für Heizungssteuerung	$3,2 \cdot 10^{-2}$
K1.4	40EG01VENBR	8	Keilriemen für Kühlturmventilator	$1,5 \cdot 10^{-1}$
K2.1	TY1741DC03BVL	11	Meßumformer für Regelung Kocherkühlung	$5,5 \cdot 10^{-1}$
K2.2	TE1741DC03BV	11	Temperaturmessung für Kühlungsregelung	$6,1 \cdot 10^{-2}$
K3.1	TV1741169BVL	11	Regelventil für Kühlungsregelung	$2,5 \cdot 10^{-1}$
K3.2	TIC1741169BVL	11	Regler für Kühlungsregelung	$3,9 \cdot 10^{-1}$
K4.1	LCV0200760EN	8	Schwimmergesteuertes Einspeiseventil	1,7
K4.2	4001840022LE	8	Leckage im Kühlkreislauf	$2,5 \cdot 10^{-2}$
K4.3	40076BV	8	Einspeisewasser	1,0
K5	40GA04ABV	8	Betriebliche Kaltwasserförderpumpe	$3,9 \cdot 10^{-1}$
K6	41GDM2ABV	9	Ventilatormotor für Gasabzug	$1,8 \cdot 10^{-1}$
K7.1	41GD02AKR	9	Keilriemen für Ventilator	$1,5 \cdot 10^{-1}$
K7.2	41113BL	9	Absorption	$1,8 \cdot 10^{-2}$
K8	41GF03BR	11	Rührerachse	$3,5 \cdot 10^{-3}$
K9.1	41GF03BV	11	Hydraulikmotor für Rührer	$8,8 \cdot 10^{-3}$
K9.2	41GS02BV	11	Hydraulikversorgung für Rührer	$7,0 \cdot 10^{-2}$

Die Schlüssel beziehen sich auf die Fehlerbäume der Bilder 6.11 bis 6.14.

- Explosion im Kocher (Fehlerbaum 11, Bild 6.14); zugehörige Teilfehlerbäume:
  - Fehlerbaum 8 (Bild 6.11): Ausfall des Wasserkühlkreislaufs (für Kühlung des Kochers)
  - Fehlerbaum 9 (Bild 6.12): Ausfall des Gasabzugs des Kochers

Tab. 6.6:

Auslösende Ereignisse und ihre Eintrittshäufigkeiten für den Ausfall des hydraulischen Transportsystems

Störfallauslösende Ereignisse				Häufigkeit des auslösenden Ereignisses $s_j(a^{-1})$
Ereignis Nr.	Ausgefallene Komponente für das auslösende Ereignis			
	Schlüssel des Fehlerbaumeingangs	Fehlerbaum	Bezeichnung	
T1.1	LC42DF02BVL	12	Regler für Ablaufregelung	1,7
T1.2	LV0342016BVL	12	Regelventil LV 03 fällt aus	$5,0 \cdot 10^{-1}$
T1.3	LV0342016DLA	12	Druckluftversorgung für Regelventil	$5,7 \cdot 10^{-1}$
T2	XV01A41117AU	12	Automatische Umschaltung	$2,6 \cdot 10^{-2}$
T3	42GA02ABV	12	Förderpumpe zur Vorlage	$7,7 \cdot 10^{-1}$
T4	42GA03ABV	12	Förderpumpe (Förderkreislauf)	$3,9 \cdot 10^{-1}$
T5	42021BR	12	Bruch der Förderleitung	$8,8 \cdot 10^{-4}$
T6	XV01A41117SNU	12	Dreiwegeventil	$8,8 \cdot 10^{-1}$
T7	SV0841102BV	12	Motorventil SV 08	$1,4 \cdot 10^{-1}$
T8	LSLH04BV	12	Niveaumesser im Aufgabetrichter	$5,0 \cdot 10^{-2}$
T9	OP42DF02NE	12	Auslauf des Separiergeräts verstopft	$2,7 \cdot 10^{-3}$

Die Schlüssel beziehen sich auf den Fehlerbaum des Bildes 6.15.

- Fehlerbaum 10 (Bild 6.13): Ausfall "Entleerungssystem Kocher" (ohne Auslösung)

- Ausfall des hydraulischen Transportsystems (Fehlerbaum 12, Bild 6.15)

Nachfolgend werden die einzelnen Fehlerbäume kurz beschrieben und die Annahmen, die bei ihrer Erstellung getroffen wurden, dargestellt.

6.2.2 Fehlerbäume

Die Fehlerbäume der Abbildungen 6.4 bis 6.15 sind der Übersichtlichkeit halber in die drei Ebenen Steuerung, Energieversorgung und Verfahrenstechnik (von links nach rechts, wobei

nicht besetzte Ebenen entfallen) unterteilt. Bezüglich der Bedeutung dort angewandter Bildzeichen für die Funktionselemente und der Verknüpfungsarten wird auf Kapitel 4 verwiesen.

Zum allgemeinen Verständnis der Fehlerbäume erfolgt hier eine kurze Beschreibung der Überlegungen, die ihrer Erstellung zugrunde liegen. Dabei werden Gedanken und Annahmen, die für die Fehlerbäume allgemein gelten, der Beschreibung der einzelnen Fehlerbäume vorangestellt.

In den betrachteten Systemen tritt bei der Schaltung der Pumpen jeweils die gleiche Kombination von Betriebs- und Reservekomponenten auf. Die Anordnung der Pumpen erfolgt immer nach dem gleichen Schema. Der Förderstrang verzweigt sich vor der Pumpe in zwei parallele Stränge mit jeweils einer Pumpe gleichen Typs, die gegen Rückströmung durch eine Rückschlagklappe gesichert ist. Außerdem ist jeder Strang durch mindestens eine Handarmatur absperrbar (Bild 6.2). In Betrieb befindet sich jeweils nur eine Pumpe, wobei dies die Pumpe A oder B sein kann.

Zum Ausfall der bestimmungsgemäßen Förderung führen bei dieser Anordnung folgende Ausfallkombinationen (Fehlerbaum 1, Bild 6.4):

- Ausfall der betrieblichen Förderpumpe und Ausfall der bestimmungsgemäßen Förderung mit der Reservepumpe. Diese können ausfallen, wenn
  - die Pumpe nicht startet (Wegen der kurzen Betriebszeit der Reservepumpe im Störfall kann die Ausfallart "Pumpe fördert nicht" gegenüber dem Startversagen vernachlässigt werden.);
  - die Pumpe nicht gestartet wird, weil die Notwendigkeit hierzu nicht erkannt wird;
  - die Rückschlagklappe hinter der Betriebspumpe nicht schließt und das Handventil vor der Betriebspumpe bei Ausfall der Rückschlagklappe als Ersatzmaßnahme nicht geschlossen wird (Bei offener Rückschlagklappe wird

sonst rückwärts über die defekte Betriebspumpe im Kreis gefördert.);

- die Rückschlagklappe hinter der Reservepumpe nicht öffnet (Dieser Ausfall kann nicht durch eine Handmaßnahme korrigiert werden, da die Rückschlagklappe nicht von Hand geöffnet werden kann.).

Aufgrund der symmetrischen Anordnung der beiden Pumpen ist es für die Analyse unerheblich, welche als Betriebs- und als Reservepumpe gewählt wird. Für die Fehlerbaumanalyse wurde festgelegt, daß Pumpe A die Betriebspumpe und Pumpe B die Reservepumpe ist. Außerdem wurden noch die folgenden wesentlichen Festlegungen getroffen:

- Es wird davon ausgegangen, daß die Handventile vor und hinter der Reservepumpe offen sind und dies wöchentlich vor Betriebsbeginn überprüft wird.
- Es wird entsprechend der Aussage des Betreibers davon ausgegangen, daß beim Ausfall von betrieblichen Komponenten und Umschalten auf Reservekomponenten die Anlage mit der Reservekomponente nur noch so lange weiterbetrieben wird, wie es für ihr betriebliches Abfahren erforderlich ist, d.h., bei der Reservepumpe entfällt ein Ausfall durch Wartung, Reparatur oder Betriebsversagen.
- Konservativ wird unterstellt, daß sogar bei kleinen Ausfällen in der für Gegenmaßnahmen zur Verfügung stehenden Zeit eine Wiederherstellung einer ausgefallenen Komponente durch Reparatur nicht möglich ist, d.h., eine einmal ausgefallene Komponente bleibt für die gesamte Dauer eines Störfalles nicht verfügbar.
- Bei allen Komponenten wird davon ausgegangen, daß sie so gewartet werden, daß keine Verschleißausfälle auftreten, sie also durch eine konstante Ausfallrate beschrieben werden können (Kapitel 5).
- Bei Störungen, die eine Explosion im Nitrierer bewirken können, kann der Inhalt des Nitrierers in einen Notablaßtank entleert werden. Da nicht abgeschätzt werden kann, wie

sich das Hexamin, wenn es nicht gleichzeitig mit dem Ablassen gestoppt wird, im entleerten, aber noch feuchten Nitrierer verhält, wird in der Analyse konservativ davon ausgegangen, daß zum erfolgreichen Ablassen ein erfolgreiches Stoppen der Hexaminzufuhr gehört. Das heißt, das Ablassen alleine reicht nicht aus, um eine Explosion zu verhindern.

- Bei Ausfall des Rührers im Nitrierer oder Kocher können örtliche Überhitzungen auftreten, die nicht sicher detektiert werden können. Deshalb wurde konservativ davon ausgegangen, daß bei der Temperaturüberwachung der Reaktoren dieser Störfall nicht entdeckt wird und somit nur Handmaßnahmen aufgrund der Drehzahlalarme der Rührer als Gegenmittel zur Verfügung stehen.
- Es wird unterstellt, daß sich nur fachkundiges Personal in der Anlage aufhält; Sabotage wird nicht betrachtet. Dies bedeutet, daß unbeabsichtigte oder beabsichtigte falsche Maßnahmen nicht berücksichtigt werden.

6.2.2.1 Fehlerbäume 1-3: Ausfall der Nitriererkühlung

Für die Fehlerbaumanalyse wird der Ausfall der Nitriererkühlung zweckmäßig untergliedert in die Ausfälle der folgenden Systemteile:

- warmer Teil des Kühlmittelkreislaufes (Fehlerbaum 1, Bild 6.4)
- kalter Teil des Kühlmittelkreislaufes (Fehlerbaum 2, Bild 6.5)
- Kühlungsregelung am Nitrierer (Fehlerbaum 3, Bild 6.6).

Ausfälle in diesen Teilen der Nitriererkühlung führen, wenn sie unentdeckt bleiben bzw. dagegen nichts getan wird, zum Ausfall der Kühlung des Nitrierers. Werden dann auch am Nitrierer selbst keine Gegenmaßnahmen ergriffen, so kann die Reaktion außer Kontrolle geraten, was zu einer Explosion führen kann (Abschnitt 6.1).

- Fehlerbaum 1:
  Ausfall "warmer Teil" des Kühlmittelkreislaufs (Bild 6.4)

Der warme Teil des Kühlmittelkreislaufes kann grundsätzlich auf zwei Arten ausfallen: zum einen durch alle Ausfälle, die eine Auswirkung auf den Kühlmitteldurchsatz haben, zum anderen durch solche, die zum Versagen der Kühlwirkung aufgrund von Störungen in der Rückkühlung führen. Dabei wirken sich die Ausfälle im warmen Teil der Kühlung zunächst auf deren kalten Teil aus, wie Bild 6.2 zu entnehmen ist.

Ein Versagen als Folge zu geringen Kühlmitteldurchsatzes kann auftreten durch

- gleichzeitigen Ausfall der in Betrieb befindlichen Kühlmittelförderpumpe 40GA-01A und des Alarms FAL 01 des der Förderpumpe nachgeschalteten Durchflußmessers oder durch Nichtbeachten dieses Alarms, so daß der Pumpenausfall nicht bemerkt und deshalb die Notwendigkeit von Gegenmaßnahmen nicht erkannt wird;
- Ausfall der Kombination Betriebspumpe 40GA-01A/Reservepumpe 40GA-01B entsprechend den oben genannten Ausfallkombinationen und Ausfall der Handabschaltung des Nitrieres (Übertrag aus Fehlerbaum 5) als alternative Maßnahme, wenn beide Förderpumpen versagen.

Des weiteren kann eine unbemerkte Leckage im warmen Teil des Kühlkreislaufs einschließlich Kühlmitteltank, die so liegt, daß sie durch den Durchflußalarm FAL 01 nicht gemeldet wird (hinter dem Durchflußmesser), zu ungenügendem Kühlmitteldurchsatz führen.

Alle vorgenannten Ausfälle bewirken ein allmähliches Entleeren des kalten Teiles des Kühlmitteltanks, das auch bei vollständigem Ausfall der Einspeisung erst nach einer Stunde beendet ist. In Anbetracht dieser langen zur Verfügung stehenden Zeit gibt es eine gewisse Wahrscheinlichkeit dafür, daß bei einem Kontrollgang das Entleeren des Tankes (örtlicher Füllstands-

anzeiger) oder das Leck entdeckt wird. Dies wurde deshalb als Funktionselement in den Fehlerbaum aufgenommen.

Ein Versagen aufgrund zu hoher Kühlmitteltemperaturen kann dadurch auftreten, daß die Rückkühlung des Kühlmittels durch die Kältemaschine ausfällt. Dies kann geschehen, wenn

- das Rückkühlsystem (Kältemaschine, nur einmal vorhanden) oder der Thermostatschalter TS 4001 für das Rückkühlsystem in ausgeschalteter Stellung ausfällt, und
- der Temperaturalarm TAH 04 (Meßstelle im kalten Kühlkreis) bei Überschreiten der eingestellten Grenztemperatur des Kühlmittels keinen Alarm gibt, der Alarm nicht beachtet wird oder keine Abhilfemaßnahmen (Abschalten des Nitrierers, Übertrag aus Fehlerbaum 5) getroffen werden.

Die vorgenannten Versagensarten wirken sich auf zwei verschiedene Weisen auf den Nitrierer aus. Ausfälle, die den Durchsatz des Kühlmediums betreffen (Pumpenausfälle, Leckagen), wirken sich, wenn sie unentdeckt bzw. ohne Gegenmaßnahmen bleiben, zuerst auf den kalten Teil des Kühlkreislaufs aus (Entleerung des kalten Kühlmitteltankes) und erst nach dessen Ausfall tritt eine Auswirkung auf den Reaktor ein. Ein Ausfall der Rückkühlung bewirkt unmittelbar einen Anstieg der Temperatur des Kühlmittels im kalten Teil des Kühlkreislaufs. Wird der Anstieg dort nicht entdeckt bzw. werden keine entsprechenden Gegenmaßnahmen ergriffen, ist es nicht mehr möglich, Auswirkungen auf den Nitrierer zu verhindern.

Zusätzlich zu den oben schon genannten allgemeinen Annahmen wurden bei der Erstellung des Fehlerbaumes 1 noch folgende spezielle Annahmen zugrunde gelegt:

- Die warme und kalte Seite des Kühlmittelbehälters werden jeweils als unabhängige Behälter betrachtet.
- Wegen des geringen Druckes werden in den Leitungen und Behältern des Kühlmittelkreislaufes nur Leckagen, aber kein totales Versagen (z.B. Leitungsabriß, Behälterbersten) unterstellt.

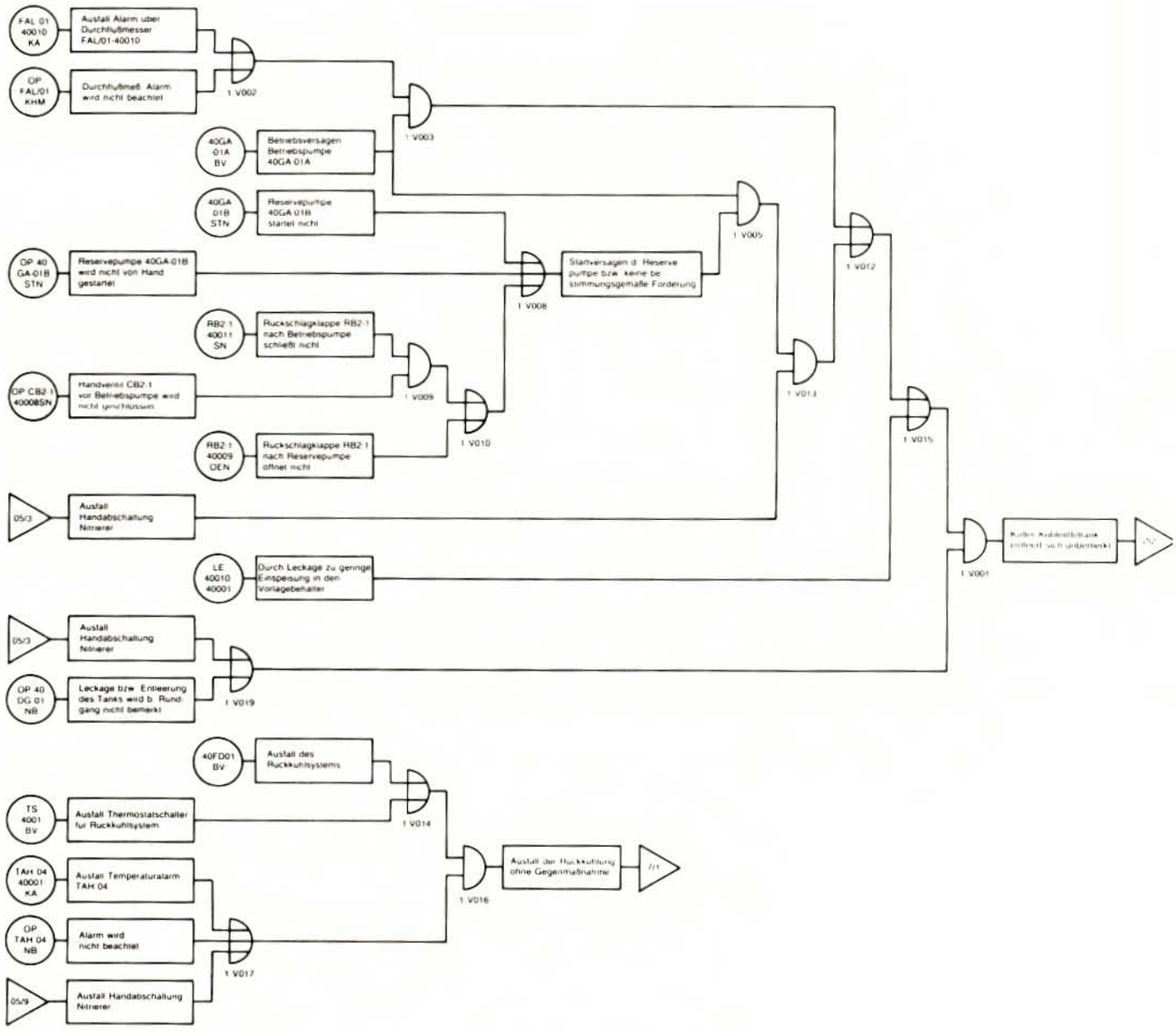


Bild 6.4:

Fehlerbaum 1: Ausfall "warmer Teil" des Kühlmittelkreislaufs

- Fehlerbaum 2:
  Ausfall der Solekühlung (gemeinsamer "kalter Teil") und Ausfall der Abschaltung der Hexaminzufuhr bei Kühlungsausfall (Bild 6.5)

Zum Ausfall des kalten Teils des Kühlmittelkreislaufes können Komponentenausfälle führen, die eine Verminderung bzw. einen Ausfall des Kühlmitteldurchsatzes bei gleichzeitigem Ausfall von eventuell möglichen Gegenmaßnahmen bewirken. Folgende Ausfallkombinationen sind denkbar:

- Rohrleckage hinter dem Druckschalter PSL 07 bzw. Alarm PAL 06. Diese kann in der Regel nicht rechtzeitig entdeckt werden (Detektion erst durch "Niveau-Alarm niedrig" im warmen Teil des Kühlmittelbehälters). Die Leckage muß dabei jedoch so groß sein, daß die ausreichende Versorgung aller Verbraucher nicht mehr gesichert ist.
- Ausfall der Betriebspumpe 40GA-02A und nicht bestimmungsgemäße Förderung mit der Reservepumpe 40GA-02B oder unbemerktes Entleeren des kalten Kühlmitteltanks (Übertrag aus Fehlerbaum 1), wenn in beiden Fällen weder über den Druckschalter PSL 07 die Hexaminzufuhr gestoppt wird noch aufgrund des Alarmes PAL 06 Gegenmaßnahmen getroffen werden (Abschalten der Hexaminzufuhr von Hand).

Der Ausfall der Betriebspumpe des kalten Teils 40GA-02A und die nicht bestimmungsgemäße Förderung durch die Reservepumpe 40GA-02B sind auf die gleiche Art wie eingangs allgemein beschrieben möglich. Außerdem kann es sein, daß als Folge eines Ausfalls des Alarms PAL 06 oder aufgrund seiner Nichtbeachtung die Reservepumpe nicht in Betrieb genommen wird.

Die Abschaltung der Hexaminzufuhr über den Druckschalter PSL 07, die bei Unterschreiten eines Sollwertes automatisch erfolgen soll, kann ausfallen, wenn

- vom Druckschalter kein Abschaltsignal an die Hexameinspeisung "7" gegeben wird oder

- der Schalter, über den die Hexaminzufuhr gestoppt werden soll, trotz anstehenden Signals nicht abschaltet.

Die Abschaltung der Hexaminzufuhr von Hand, die aufgrund eines Alarms von PAL 06 möglich wäre, erfolgt nicht, wenn

- der Alarm PAL 06 ausfällt oder nicht beachtet wird;
- die Handmaßnahme "Hexamin stoppen" trotz Alarm unterbleibt und auch aus der Tatsache, daß die Betriebsanzeige der Hexaminförderung deren Weiterbetrieb anzeigt, kein Rückschluß darauf erfolgt, daß die Förderung abgeschaltet werden muß;
- sich die Zufuhr von Hexamin als Folge eines Schalterversagens nicht abstellen läßt (jeweils ein Schalter für automatisches Abschalten und Abschalten von Hand).

Für Maßnahmen bei Störungen im kalten Teil des Kühlmittelkreislaufes steht eine relativ kurze Zeitspanne zur Verfügung (ca. 10 Minuten), da die Temperatur im Nitrierer als Folge von Ausfällen in diesem Teil der Kühlmittelversorgung sehr schnell ansteigt.

Folgende spezielle Annahmen wurden bei der Erstellung des Fehlerbaumes getroffen:

- Es wird vorausgesetzt, daß ein Abschalten der Hexaminzufuhr ausreicht, um eine Explosion zu verhindern, so daß der Reaktorinhalt nicht unbedingt in den Notablaßtank eingeleitet werden muß. Die Abschaltung kann dabei über den Druckschalter PSL 07 oder von Hand aufgrund eines Alarms durch PAL 06 erfolgen. Sollten beide Möglichkeiten ausfallen, so steht dann allerdings als zusätzliche Maßnahme noch das Notablassen zur Verfügung.
- Die Hexamineinspeisung kann durch Abschalten der Förderschnecke "7" gestoppt werden.

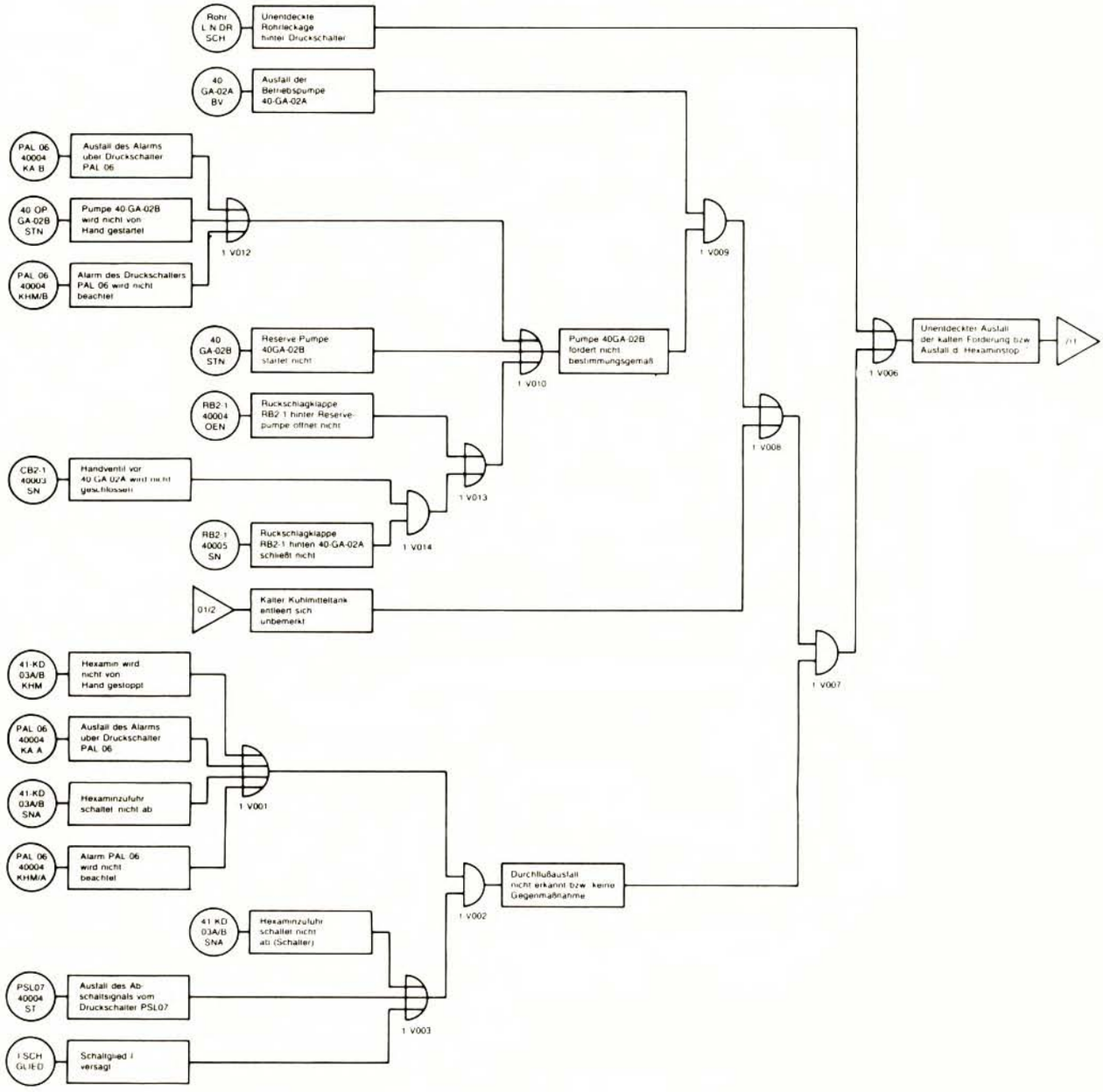


Bild 6.5:

Fehlerbaum 2: Ausfall der Solekühlung (gemeinsamer "kalter Teil") und Ausfall der Abschaltung der Hexaminzufuhr bei Kühlungsausfall

- Fehlerbaum 3:
  Ausfall der Kühlungsregelung Hauptnitrierer (Bild 6.6)

Bei funktionierender Kühlmittelversorgung aus dem gemeinsam warmen und kalten Teil kann die Kühlung des Nitrierers wie folgt versagen:

- Ausfall des Reglers TIC 07A oder des Regelventils TV 07 für die Durchflußregelung der Kühlschlangenkühlung derart, daß der Durchfluß geringer als erforderlich ist bei gleichzeitigem Nichtöffnen des Bypassventils zum Regelventil TV 07A;
- Ausfall der Temperaturmessung oder des Meßumformers für d Kühlungsregelung dergestalt, daß beide eine geringere Temperatur als tatsächlich vorhanden vortäuschen.

Das Öffnen der Bypassleitung, mit der der Ausfall des Regelventils überbrückt werden kann, muß von Hand vor Ort erfolgen Es steht im Extremfall nur die sehr kurze Zeitspanne von ca. 10 Minuten zur Verfügung, bis im Nitrierer infolge der unzureichenden Kühlung unkontrollierte Zustände eintreten. Das Öffnen des Bypassventils unterbleibt, wenn der Alarm "Temperatur im Nitrierer hoch" nicht gegeben wird, d.h. bei Ausfall des Alarmgebers TAH 07A oder bei Alarm "Temperatur hoch" das Bypassventil in der verfügbaren Zeit nicht betätigt wird (da der Regler bzw. das Regelventil als Ursache der Störung nicht erkannt wird), oder das Bypassventil sich nicht öffnen läßt. Ein Ausfall in Richtung niedrige Temperatur beim Temperaturmeßgerät TE 07A, an dem die Kühlungsregelung (bewirkt ein Zufahren der Regelarmatur) und der Alarm "Temperatur hoch" angeschlossen sind, führt direkt zur unzureichenden Kühlung des Nitrierers. Den gleichen Effekt hat ein entsprechender Ausfall des pneumatischen Temperaturmeßumformers TY 07A, der dem Regler und dem Alarmgerät vorgeschaltet ist, da in diesem Fall - wie auch beim Ausfall von TAH 07A - unbekannt ist, daß der Bypass geöffnet werden müßte. Als Gegenmaßnahme bleibt dann nur das automatische Hexaminstoppen und Ablassen, die beide von den Temperaturwächtern mit den Grenzwertschaltern

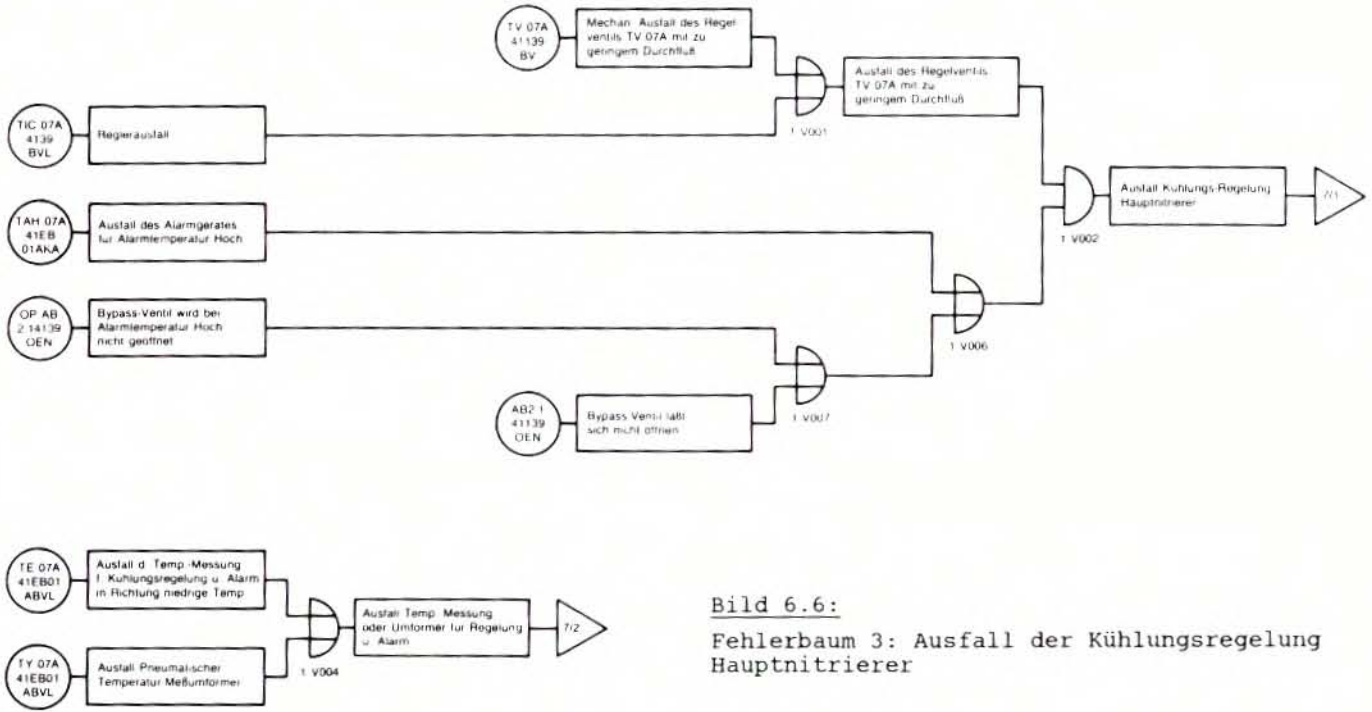


Bild 6.6:

Fehlerbaum 3: Ausfall der Kühlungsregelung Hauptnitrierer

TSH 08A und TSHH 08A (siehe Fehlerbäume 5 und 6) ausgelöst werden.

Fehler in den Steuerleitungen wie Bruch der Leitung zwische Meßgerät und Umformer sowie der Lüftungsleitung nach dem Um former führen wegen des "fail safe"-Prinzipes zum vollen Öff nen des Regelventils und damit nicht zu einer Beeinträchti- gung der Kühlung, so daß diese Ausfälle nicht betrachtet wer den müssen.

Konservativ wurde bei der Fehlerbaumerstellung angenommen, da die Mantelkühlung allein nicht zur Kühlung des Nitrierers aus reicht.

6.2.2.2 Fehlerbaum 4:
Ausfall der Salpetersäureversorgung (Bild 6.7)

Heftige Reaktionen im Nitrierer (mit möglicher Folge einer Explosion) können auftreten, wenn die Menge der eingespeisten Salpetersäure im Verhältnis zum zugeführten Hexamin zu klein wird oder die Salpetersäureeinspeisung ganz ausfällt, ohne daß Gegenmaßnahmen ergriffen werden (Abschnitt 6.1). Das Ausbleiben der Hexaminzufuhr ist demgegenüber ein sicherheitsgerichtetes Ereignis. Aus diesem Grund wird es z.B. für Gegenmaßnahmen bei Störfällen ausgenutzt.

Das für den Prozeß optimale Salpetersäure/Hexamin-Verhältnis wird beim Anfahren der Anlage nach dem Betriebshandbuch aufgrund von Erfahrungswerten eingestellt und über Durchflußmesser (Rotameter) angezeigt, mitgeschrieben und überwacht. Die Einstellung der eingespeisten Hexaminmenge erfolgt über die Drehzahl der Einspeiseschnecke. Ein fälschliches Höherstellen der Hexaminzufuhr wird nicht unterstellt (vgl. allgemeine Annahmen im Abschnitt 6.2.2), so daß eine Verringerung des Verhältnisses von Salpetersäure zu Hexamin nur durch einen Ausfall der Salpetersäureeinspeisung in den Nitrierer infolge Ausfalls der Einspeisepumpen zustande kommen kann. Wegen der

ır redundanten Sicherheitseinrichtungen in der Salpetersäu-
'ersorgung sind Störungen mit Auswirkungen in diesem Bereich
lerdings so unwahrscheinlich, daß sie praktisch keinen Ein-
ıß auf das Ergebnis haben. Deshalb wurde auf die Einbezie-
ng weiterer auslösender Ereignisse (z.B. Leckage in der För-
rleitung oder Leckage des Salpetersäuretagestankes), die
ch unwahrscheinlicher sind als ein Pumpenausfall und das Er-
bnis nur geringfügig ändern würden, verzichtet.

.e Einspeisung der Salpetersäure wird als ausgefallen angese-
en, wenn die betriebliche Säureeinspeisepumpe 41GA-01A nicht
ınktionsfähig ist und die bestimmungsgemäße Förderung durch
ie Reservepumpe 41GA-01B aufgrund fehlenden Erkennens des
alpetersäureausfalls (Beschreibung weiter unten) oder eines
usfalles bei der Inbetriebnahme der Reservepumpe ausbleibt.
Die Ausfallmöglichkeiten wurden eingangs allgemein beschrie-
)en.)

)ie beim Ausfall der Säureeinspeisung möglichen Handmaßnahmen
)zw. die dafür vorgesehenen Sicherheitsschaltungen versagen,
wenn

- die automatische Abschaltung der Hexaminzufuhr ausfällt, wobei entweder alle drei zur Abschaltung vorgesehenen Signale ausfallen müssen, nämlich der Abschaltbefehl bei Ausfall der betrieblichen Einspeisepumpe, das Abschaltsignal vom Durchflußmesser FSL 02A und das Abschaltsignal vom Niveaumesser LSL 04 im Vorlagebehälter, oder trotz anstehenden Abschaltsignals die Hexaminzufuhr nicht abschaltet (Schalterversagen);
- das Schaltglied I versagt, wobei dann ein Common-Mode-Ausfall vorläge, da keines der im vorangehenden Punkt genannten Anregungssignale zur Abschaltung führen würde;
- der Nitrierer nicht von Hand abgeschaltet wird als Folge des Ausfalls "Alarm Durchfluß niedrig" FAD 01 des ersten Rotameters und des "Niveau-Alarms niedrig" LAL 04 im Vorlagebehälter "2" oder infolge eines Nichtbeachtens dieser beiden Alarme (diese Ausfallkombinationen führen auch dazu,

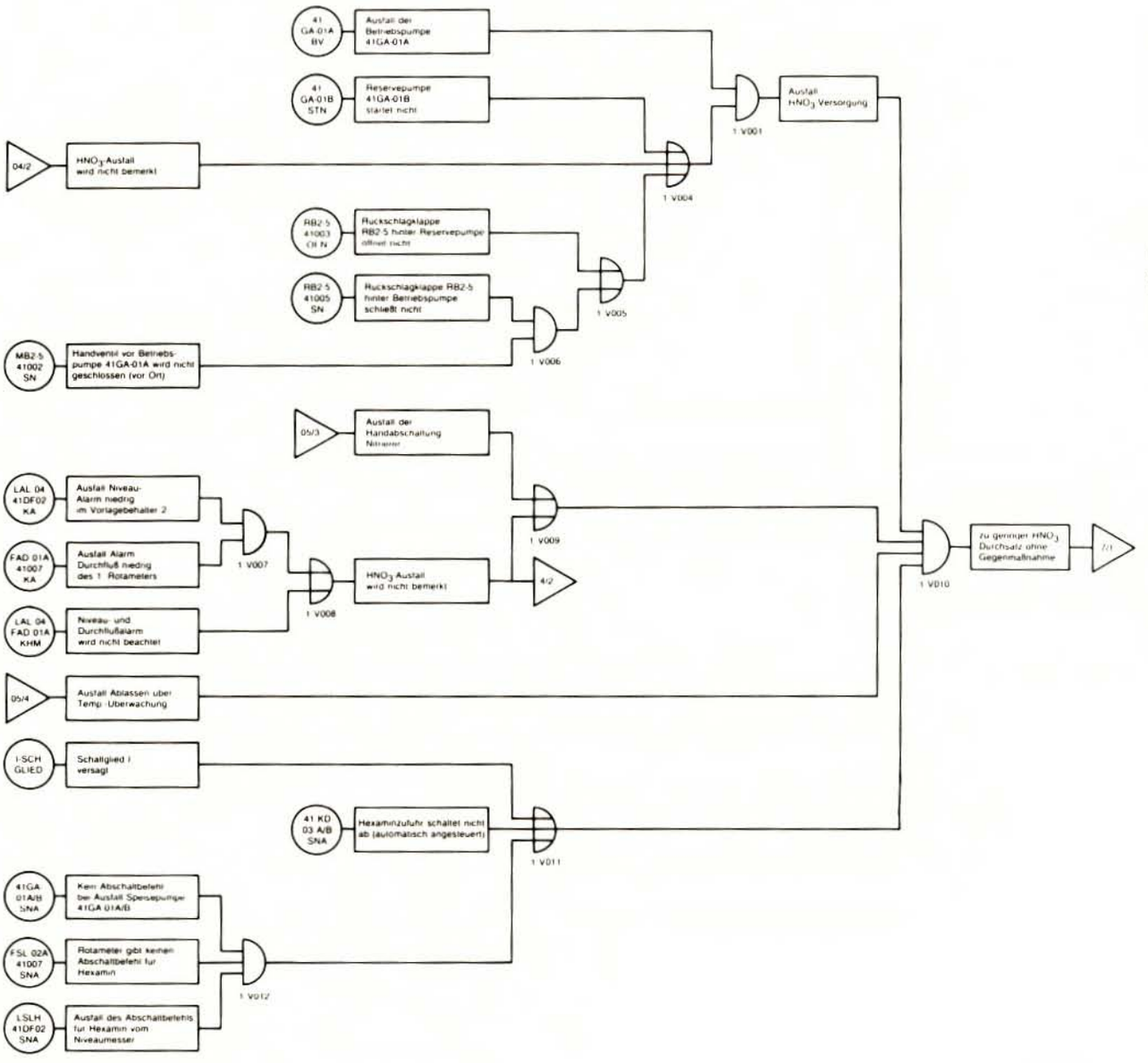


Bild 6.7:

Fehlerbaum 4: Ausfall der Salpetersäureversorgung

daß die Reservepumpe nicht gestartet wird (Übertrag 4/2)) oder weil der Nitrierer nicht von Hand abgeschaltet wird (Übertrag aus Fehlerbaum 5);

- als letzte Maßnahme das Ablassen des Nitrierers über die Temperaturüberwachung versagt (Übertrag aus Fehlerbaum 5).

6.2.2.3 Fehlerbaum 5:
Ausfall "Ablassen bzw. Abschalten des Nitrierers"
(Bild 6.8)

Wie bereits erwähnt, muß der Nitrierer bei bestimmten Störungen oder Ausfällen in seinen Versorgungs- bzw. Regelsystemen zur Vermeidung eines Durchgehens der Reaktion, das zur Explosion führen kann, durch geeignete Maßnahmen in einen sicheren Zustand überführt werden. Entsprechend dem Ereignisablauf bis zu dem Moment, in dem der Nitrierer entleert werden muß, sind mehrere Fälle mit unterschiedlichen möglichen Maßnahmen zu betrachten.

Für das Ergreifen von Maßnahmen kann eine längere Zeit verfügbar sein, z.B. beim Ausfall des warmen Teils des Kühlmittelsystems oder beim Ausfall der Salpetersäureversorgung. Dann reicht es aus, die Hexaminzufuhr abzuschalten. Das Notablassen des Nitrierers ist schließlich die letzte Maßnahme, die nach dem Versagen einer Reihe vorgeschalteter Eingriffe zur Verfügung steht. Dies wird in den Teilfehlerbäumen "Ausfall Handablassen Nitrierer, Fall A" und "Ausfall Handabschaltung Nitrierer" dargestellt, wobei im zweiten Teilfehlerbaum der erste durch Übertrag enthalten ist. Der erste Teilfehlerbaum wird auch zur Beschreibung des Ausfalls des Handablassens bei Anstehen des Temperaturalarmes TAH 07A verwendet.

Bei Ausfall des Rührers steht für Gegenmaßnahmen nur eine sehr kurze Zeit zur Verfügung, da hier örtliche Überhitzungen mit der Folge eines Durchgehens der Reaktion auftreten können. In diesem Fall ist das rechtzeitige Ablassen des Reaktorinhaltes

in den Notablaßtank durch Handauslösung die einzige mögliche Maßnahme, eine Explosion zu verhindern. Dies ist im Teilfehlerbaum "Ausfall Handablassen Nitrierer, Fall B" dargestellt.

Das Handablassen des Nitrierers (Fälle A und B, die sich nur durch eine unterschiedliche Bewertung der Handmaßnahmen unterscheiden) gelingt nicht, wenn

- das dem eigentlichen Ablaßventil HV 01A vorgeschaltete Magnetventil SV 01A nicht betätigt wird; diese Maßnahme ist direkt am Ventil oder in der Warte möglich (durch Knopfdruck wird gleichzeitig der Rührer im Notablaßbehälter gestartet, so daß hierfür keine eigene Maßnahme erforderlich ist);
- das Abschalten der Hexaminzufuhr, das gleichzeitig durch den Ablaßknopf erfolgen soll, nicht funktioniert (Versagen des durch die Automatik angesteuerten Schalters);
- das Vorventil SV 01A ausfällt (z.B. durch Klemmen oder Ausfall des Druckknopfes) und das Ablaßventil HV 01A nicht von Hand vor Ort geöffnet wird (ein Versagen des Öffnens des Ablaßventils kann durch Stellungsanzeige festgestellt werden);
- das Ablaßventil HV 01A klemmt, so daß es weder über das Vorventil noch direkt von Hand über das Handrad geöffnet werden kann;
- der Rührer im Notablaßtank nicht startet.

Wie schon beschrieben, steht in einigen Fällen mehr Zeit zur Verfügung, so daß der Nitrierer durch mehrere Maßnahmen von Hand außer Betrieb gesetzt bzw. in einen ungefährlichen Zustand überführt werden kann. Es kommt dann nur zu einer Explosion, wenn

- die Hexaminzufuhr nicht gestoppt wird oder
- das Handablassen in den Notbehälter nicht erfolgt.

Es gibt also zwei Möglichkeiten, die Explosion zu verhindern.

Die Hexaminzufuhr wird nicht unterbunden, wenn die Hexameinspeisung nicht von Hand abgeschaltet wird, weil z.B. die Notwendigkeit dazu bzw. die Möglichkeit, den Störfall dadurch zu verhindern, nicht erkannt wird. Außerdem könnte es sein, daß trotz Betätigens des Handabschalters die Hexaminzufuhr beispielsweise wegen eines defekten Schalters weiterläuft.

Sollte die Hexaminzufuhr nicht abgeschaltet worden sein, bleibt als weitere Maßnahme noch das Ablassen in den Notablaßtank. Die hier zum Versagen führenden Funktionsausfälle wurden schon beschrieben.

Abgesehen vom Rührerausfall, bei dem die Detektierung eines Temperaturanstiegs im Reaktor nicht gesichert ist, kann ein Notablassen in allen anderen Fällen über die Temperaturüberwachung erfolgen. Dabei gibt es zwei Möglichkeiten: Ablassen von Hand bei Ansprechen des Temperaturalarms TAH 07A (Abschalten der Hexaminzufuhr allein reicht laut Annahme nicht aus) oder automatisch über den Temperaturschalter TSHH 08A. Beide Male wird durch das Abschaltsignal auch der Rührer im Notablaßtank eingeschaltet.

Ein Notablassen über den Temperaturalarm findet nicht statt, wenn

- der Alarmgeber TAH 07A ausfällt,
- der Alarm des Gerätes TAH 07A nicht beachtet wird oder
- die direkt das Handablassen betreffenden Funktionen ausfallen (Ausfall "Handablassen Nitrierer, Fall A").

Der Ausfall der dem Alarmgeber TAH 07A vorgeschalteten Einrichtungen (Widerstandsthermometer, pneumatischer Temperaturmeßumformer) zählt zu den auslösenden Ereignissen und wird hier nicht erneut betrachtet, da dies bereits im Zusammenhang mit dem Fehlerbaum 3 erfolgt ist.

Das automatische Ablassen über die Temperaturüberwachung kann ausfallen, wenn

- das Widerstandsthermometer TE 08A so ausfällt, daß eine Temperaturerhöhung nicht detektiert wird;
- der Grenzwertgeber TSH 08A ausfällt, so daß kein Abschaltbefehl zur Hexamineinspeisung gegeben wird;
- trotz Abschaltsignals vom Geber TSH 08A die Hexaminzufuhr nicht abschaltet;
- der Grenzwertgeber TSHH 08A so ausfällt, daß eine Temperaturerhöhung nicht rechtzeitig zu einem Ablaßsignal führt;
- das Magnetventil SV 01A für das Ablassen der Druckluft (Vorventil) zum Öffnen des Ablaßventils trotz anstehenden Öffnungssignals nicht öffnet;
- das Ablaßventil HV 01A nicht öffnet, weil es z.B. klemmt;
- der Rührer 41 GFM 08A im Notablaßtank nicht startet.

Folgende spezielle Annahmen wurden der Erstellung des Fehlerbaumes zugrunde gelegt:

- Zum Abschalten der Hexaminzufuhr ist es ausreichend, wenn die Förderschnecke abgeschaltet wird.
- Automatisches Ablassen des Nitrierers über die Temperaturüberwachung funktioniert nicht bei Rührerausfall, d.h., Handablassen ist dann die einzige wirkungsvolle Gegenmaßnahme.
- Eine Unterbrechung der Hexaminzufuhr ohne Ablassen reicht nur in folgenden Fällen aus:
  - Ausfälle im warmen Teil des Kühlmittelkreislaufes,
  - Ausfälle in der Förderung im kalten Teil des Kühlmittelkreislaufes,
  - Ausfall der Säureeinspeisung.
- Fällt beim Ablassen das gleichzeitig automatisch angeregte Hexaminstoppen aus, wird ein Abstellen des Hexamins von Hand nicht mehr als möglich erachtet. Konservativ wird dann davon ausgegangen, daß der Ablaßvorgang erfolglos war und eine Explosion nicht verhindert werden kann.

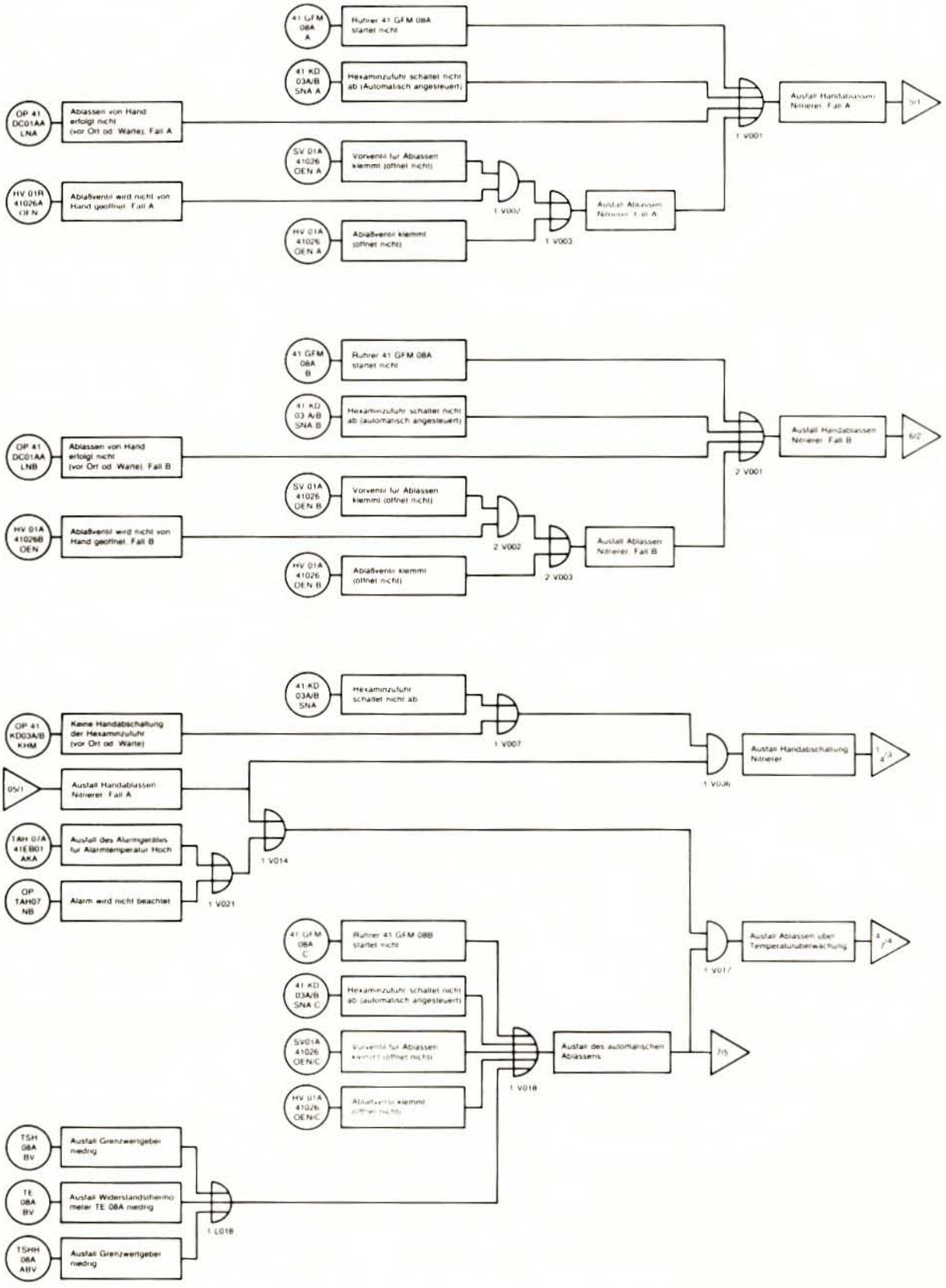


Bild 6.8:
Fehlerbaum 5: Ausfall "Ablassen bzw. Abschalten des Nitrierers"

6.2.2.4 Fehlerbaum 6:
Ausfall "Rührer des Nitrierers" (Bild 6.9)

Bei Ausfall des Rührers werden die Wärmeabfuhr und die Durchmischung schlagartig schlechter. Dadurch können örtliche Überhitzungen auftreten, die von der Temperaturüberwachung wahrscheinlich nicht entdeckt werden, so daß ein automatisches Ablassen nicht erfolgt. Das zur Vermeidung einer Explosion erforderliche Ablassen des Reaktorinhalts in den Notbehälter muß deshalb von Hand ausgelöst werden. Der Operateur kann dazu durch den Alarm "Rührerdrehzahl niedrig" (z.B. beim Ausfall des Hydraulikmotors) oder "Drehzahl hoch" (z.B. beim Bruch der Rührerwelle) veranlaßt werden. Die dann zur Verfügung stehende Zeit ist sehr kurz (< 5 min).

Das Ereignis Rührerausfall ohne Gegenmaßnahmen kann wie folgt zustande kommen:

- Bruch der Rührerwelle und Ausfall des Alarms "Rührerdrehzahl hoch" SAH 04A, Ausfall "Handablassen des Nitrierers, Fall B" (Übertrag 05/2 aus Fehlerbaum 5), obwohl auf den Alarm reagiert wird, oder Nichtbeachten des Alarms SAH 04A;
- Ausfall des Rührerantriebs als Folge eines Ausfalls des Hydraulikmotors oder der Hydraulikversorgung und Ausfall des Rühreralarms niedrig, Ausfall des Handablassens (Übertrag 05/2 aus Fehlerbaum 5, Fall B), obwohl auf den Alarm reagiert wird, oder Nichtbeachten des Alarms SAL 04A.

6.2.2.5 Fehlerbaum 7:
Explosion im Nitrierer (Bild 6.10)

In diesem Fehlerbaum sind alle Ereignisse zusammengefaßt, die zu einer Explosion im Nitrierer führen können. Dabei handelt es sich um:

- Rührerausfall ohne Gegenmaßnahmen (Übertrag aus Fehlerbaum 6),

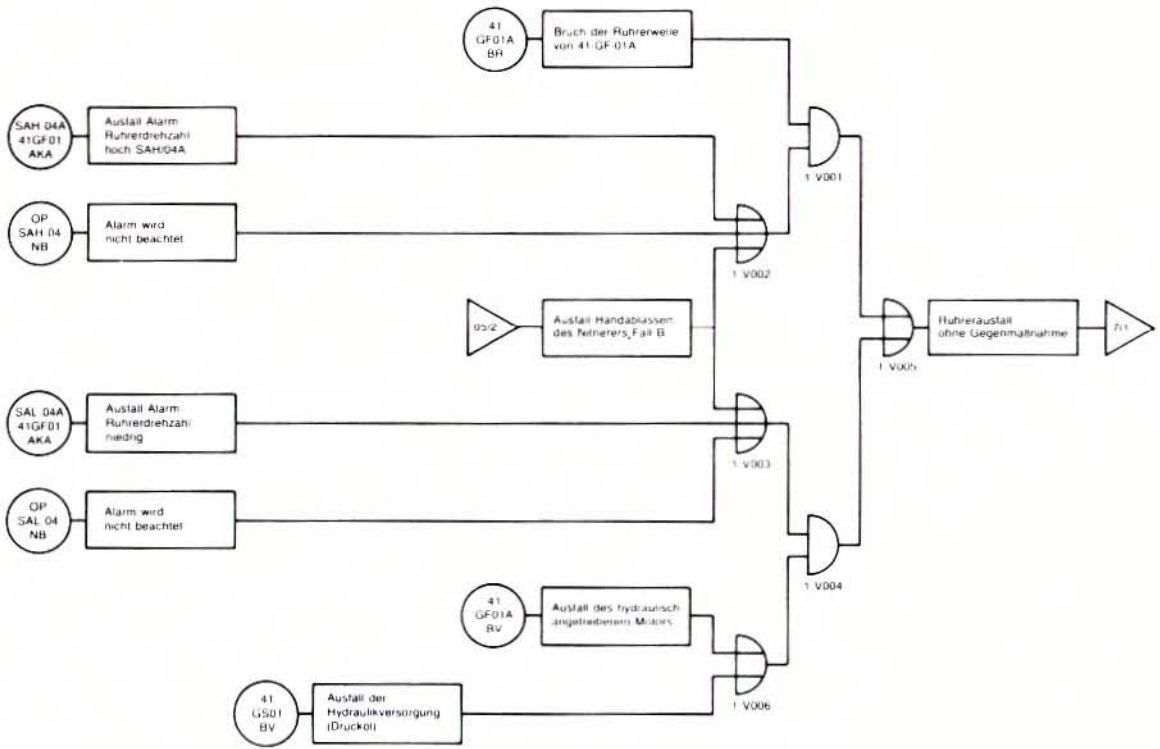


Bild 6.9:

Fehlerbaum 6: Ausfall "Rührer des Nitrierers"

- zu geringe Salpetersäureeinspeisung ohne Gegenmaßnahmen (Übertrag aus Fehlerbaum 4),
- Ausfälle in der Kühlung des Hauptnitrierers ohne Gegenmaßnahmen (Überträge aus den Fehlerbäumen 1, 2 und 3) bei gleichzeitigem Ausfall des Notablassens über die Temperaturüberwachung,
- Ausfälle in der Meßwerterfassung oder -umformung für die Temperaturregelung des Nitrierers ohne Gegenmaßnahmen (Übertrag aus Fehlerbaum 3),
- plötzliche (nicht durch vorherige kleinere Leckage angekündigte) große Leckage von Kühlmittel in den Nitrierer (aus der Kühlschlange).

  Heftige Reaktionen im Nitrierer mit der möglichen Folge einer Explosion können bei einem plötzlichen großen Leck in der Kühlschlange auftreten. Das dabei in den Reaktor eintretende Kühlmittel reagiert heftig mit der konzentrierten Salpetersäure (exotherme Reaktion), wodurch sofort eine starke, örtlich beginnende Temperaturerhöhung eintritt mit der Folge einer ungewollten Formaldehydreaktion, die zur Explosion führen kann. Der Temperaturanstieg ist so schnell, daß Gegenmaßnahmen (z.B. Ablassen durch die Temperaturüberwachung) nicht mehr sicher wirksam werden. Tritt jedoch vor dem Bruch eine kleinere Leckage auf, so ist damit zu rechnen, daß die bereits diskutierten Sicherheitsmaßnahmen (Temperaturüberwachung des Reaktors) greifen. Außerdem könnten Kühlmittelverluste über die Entleerung des Kühlmitteltankes (Niveau-Alarm im warmen Teil, örtliche Niveauanzeige an beiden Tanks) entdeckt werden (Abschnitt 6.2.2.1).

Wie schon im Zusammenhang mit dem Fehlerbaum 3 (Ausfall der Kühlungsregelung Hauptnitrierer) dargelegt, bleibt beim Eintreten des Ereignisses "Ausfall Temperaturmessung oder Meßumformer für Regelung und Alarm" (Übertrag aus Fehlerbaum 3) als einzige Gegenmaßnahme das automatische Ablassen (Übertrag 05/5 aus Fehlerbaum 5).

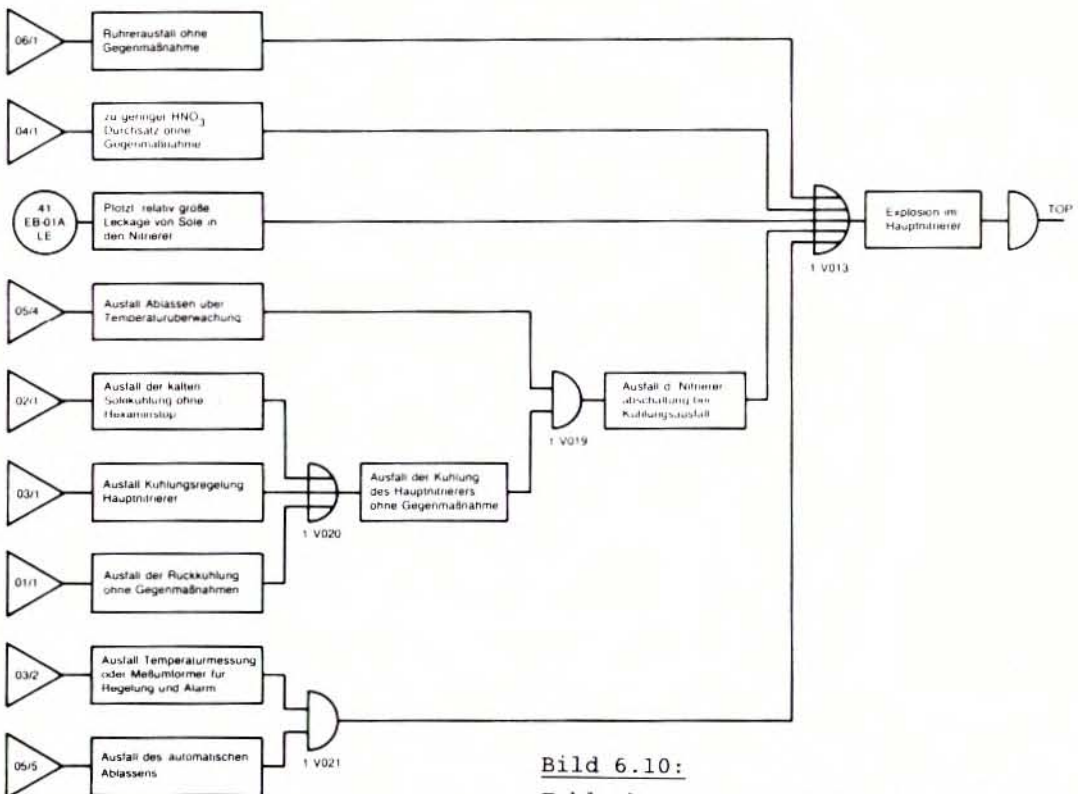


Bild 6.10:

Fehlerbaum 7: Explosion im Nitrierer

6.2.2.6 Fehlerbaum 8:
Ausfall des Wasserkühlkreislaufes (für Kühlung des Kochers) (Bild 6.11)

Fällt das Kühlsystem des Kochers ohne Gegenmaßnahmen aus, kommt es zu einem Temperaturanstieg und als Folge davon zu heftigen Reaktionen mit Gasentwicklung, so daß die Integrität des Kochers gefährdet ist. Ein unentdeckter Ausfall des Kühlwassersystems bzw. ein Ausfall ohne Gegenmaßnahmen tritt ein, wenn

- die Rückkühlung unbemerkt bzw. ohne Gegenmaßnahmen ausfällt,
- die Kaltwasser-Förderpumpen 40GA-04A/B ausfallen,
- eine Leckage im Kühlwasserkreis mit einem Leckageverlust, der größer als die maximal mögliche Einspeiserate ist, eintritt,
- die Einspeisung zur Ergänzung von Wasserverlusten ausfällt.

Das Kühlwasser, mit dem u.a. die Kocher gekühlt werden, wird über einen Naßkühlturm rückgekühlt. Fällt die Rückkühlung aus, steigt die Temperatur des Kühlwassers an. Dadurch kann es zu einer Gefährdung des Kochers kommen. Ursachen für den Ausfall der Rückkühlung können sein:

- Ausfall des Ventilators (z.B. Ausfall des Ventilatormotors; Bruch der Ventilatorwelle),
- Ausfall des Temperaturschalters TSL 07 für die Ventilatorregelung (Ventilator bleibt fälschlich ausgeschaltet),
- Ausfall des Temperaturschalters TSLL 08 für die Heizungsregelung (Heizung bleibt fälschlich eingeschaltet),
- Ausfall des Ventilators durch Keilriemenriß.

Eine gefährliche Situation tritt nur dann auf, wenn bei einem Ausfall der Rückkühlung keine Gegenmaßnahmen getroffen werden. Dies könnte aus folgenden Gründen der Fall sein:

- Das Temperaturmeßinstrument TI/05 in der kalten Leitung fällt aus.

- Die Temperaturanzeige (für die Analyse wird unterstellt, daß ein Alarm installiert wird) wird nicht beachtet.
- Gegenmaßnahmen werden in der dafür zur Verfügung stehenden Zeit (ca. 30 min) nicht wirksam.

Die Kaltwasser-Förderpumpen 40GA-04A/B können ausfallen infolge der eingangs beschriebenen Ausfallkombinationen, wobei als Signal für den Operateur der Druckmesser mit Alarm PAL 09 dient. Fällt dieser aus oder wird er nicht beachtet, werden keine Gegenmaßnahmen eingeleitet.

Des weiteren kann das Kühlwassersystem ausfallen

- wenn sich die Wasservorlage im Kühlturm unbemerkt entleert, da die Verdunstungs-, Sprüh- und Spritzverluste als Folge eines Ausfalls des schwimmergesteuerten Einspeiseventils LCV 02 nicht ergänzt werden oder kein Einspeisewasser zur Verfügung steht (das Entleeren erfolgt jedoch nur sehr langsam),
- wenn eine Leckage mit einer Ausströmrate größer als die Einspeiserate auftritt.

Für die Überwachung des Füllstandes der Wasservorlage im Kühlturm gibt es weder eine Niveauanzeige noch einen Alarm.

6.2.2.7 Fehlerbaum 9: Ausfall des Gasabzuges des Kochers (Bild 6.12)

Zur Vermeidung ungewollter Reaktionen im Kocher müssen die während des Auskochbetriebes entstehenden Gase abgezogen werden. Vor der Abgabe an die Umgebung werden die Gase in einer Gasreinigungsanlage (Absorptionskolonnen) gereinigt. Das Gasabzugsystem ist als ausgefallen zu betrachten, wenn

- der aktive Gasabzug durch die Ventilatoren ausfällt und
- die als Alternative mögliche Gasabfuhr durch Naturzug ebenfalls versagt.

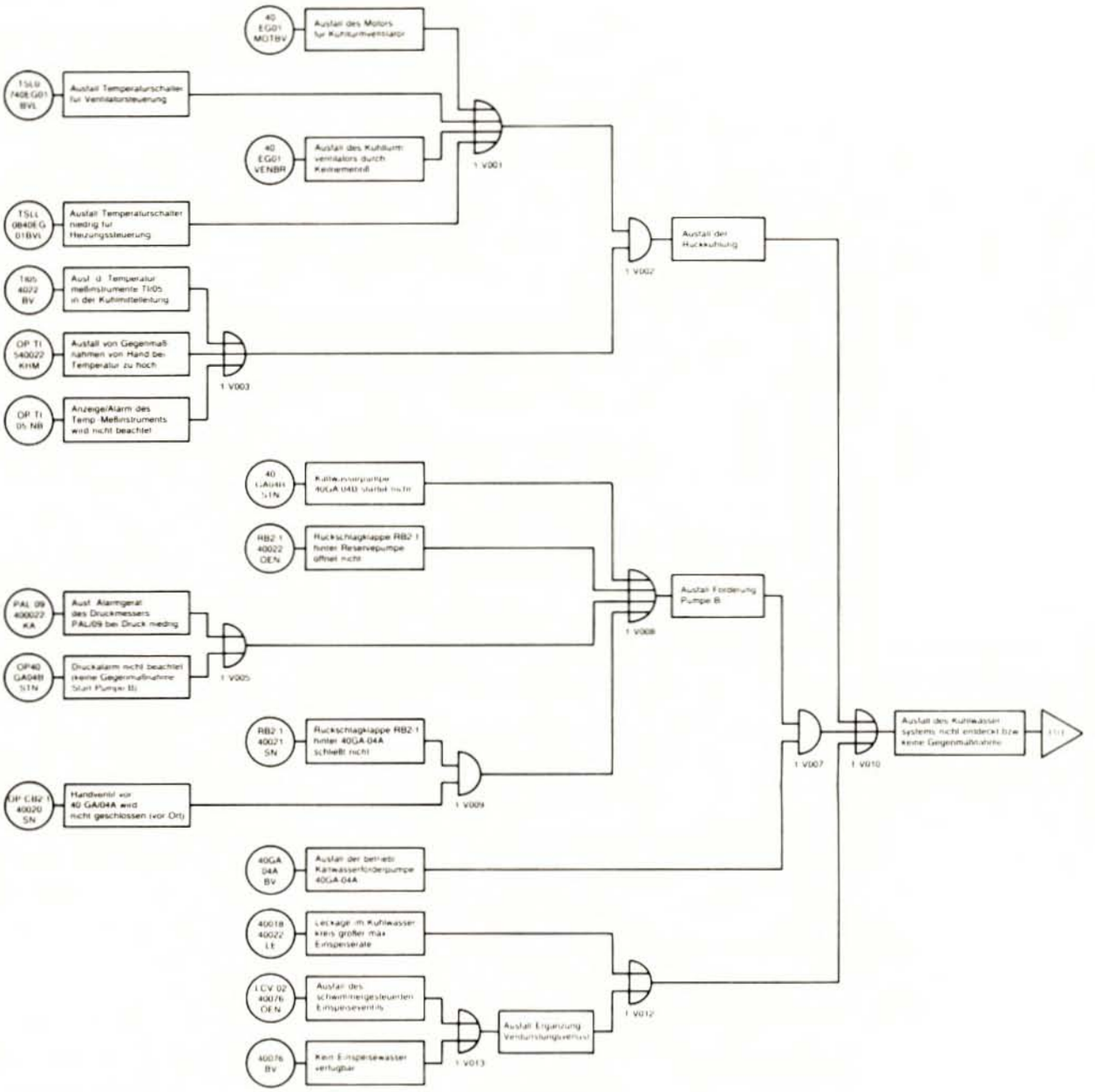


Bild 6.11:

Fehlerbaum 8: Ausfall des Wasserkühlkreislaufes (für Kühlung des Kochers)

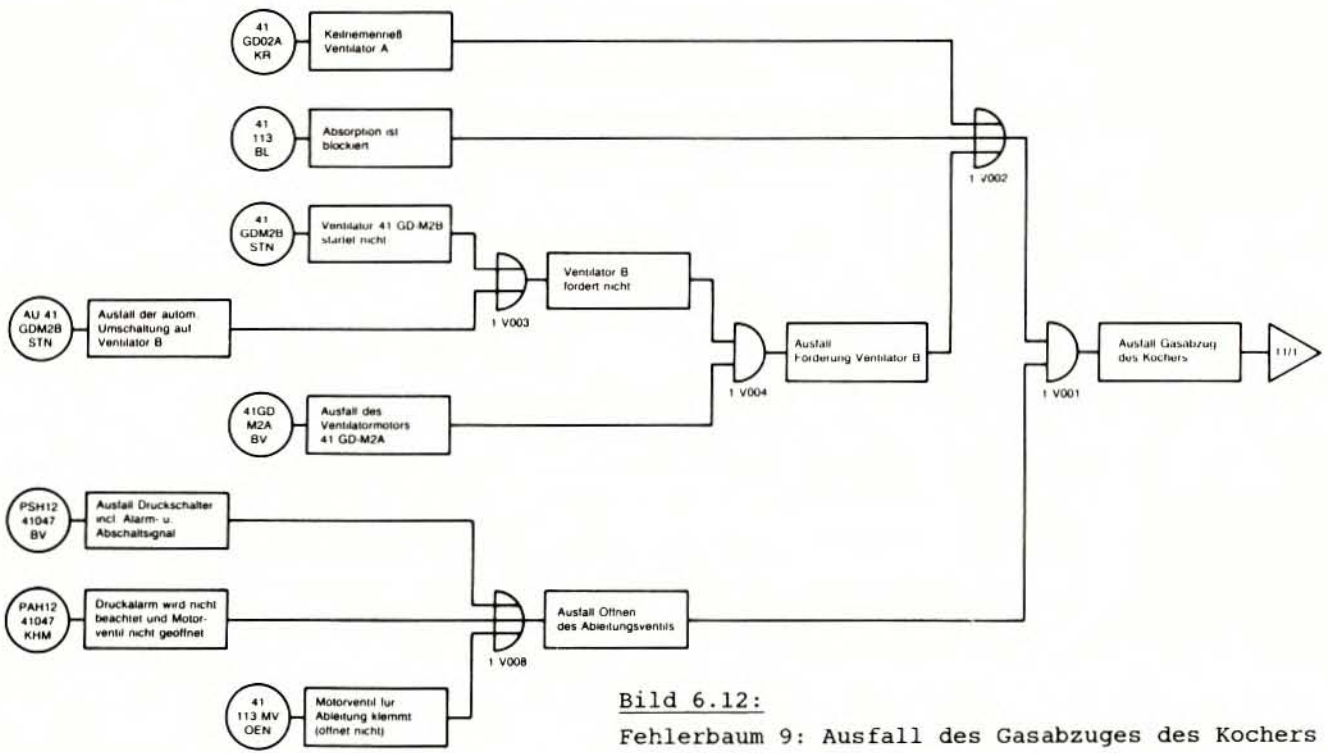


Bild 6.12:
Fehlerbaum 9: Ausfall des Gasabzuges des Kochers

Zum Ausfall des aktiven Gasabzuges führen

- ein Keilriemenriß des in Betrieb befindlichen Ventilators 41GD-02A,
- ein Blockieren der Absorption,
- ein Ausfall des Ventilatormotors 41GD-M2A und gleichzeitiger Ausfall der hierfür vorgesehenen automatischen Umschaltung auf den Reserveventilator 41GD-M2B oder dessen Startversagen.

Die alternative Möglichkeit der Abfuhr der Gase über Naturzug versagt, wenn das für die Umschaltung auf Naturzug erforderliche Ableitungsventil nicht öffnet. Dies kann dadurch eintreten, daß

- die automatische Umschaltung (automatisches Öffnen des Ableitungsventiles über Druckschalter PSH 12 bei Druckanstieg) versagt oder
- sich das Ableitungsventil (Motorventil) nicht öffnen läßt (z.B. infolge Klemmens).

6.2.2.8 Fehlerbaum 10: Ausfall "Entleerungssystem Kocher" (ohne Auslösung) (Bild 6.13)

Ähnlich wie beim Nitrierer ist auch beim Kocher als letzte Notmaßnahme das schnelle Ablassen des Reaktorinhalts in sehr kurzer Zeit in einen mit Wasser gefüllten und mit einem Rührer versehenen Notablaßbehälter vorgesehen. Die Entleerung kann sowohl von Hand als auch automatisch ausgelöst werden, wobei der Start der Rührer im Notablaßbehälter (wie beim Nitrierer) durch das Auslösen des Ablassens erfolgt. Wird das Notablassen von Hand eingeleitet, so stehen je nach dem betrachteten Ereignisablauf unterschiedliche Zeitspannen für die Auslösung zur Verfügung. Diesen Abweichungen tragen die Fenlerbäume für die Fälle A und B Rechnung, die sich durch die Wahrscheinlichkeitsbewertung der Handmaßnahmen unterscheiden. Das System fällt aus, wenn

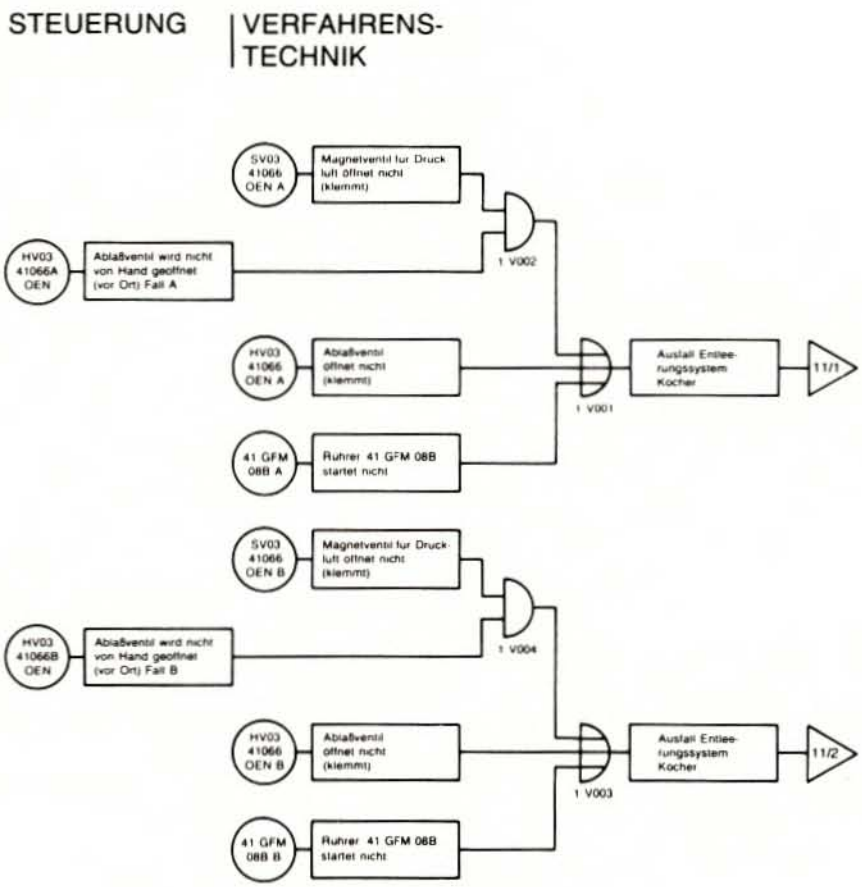


Bild 6.13:

Fehlerbaum 10: Ausfall "Entleerungssystem Kocher" (ohne Auslösung)

- das Magnetvenil SV 03, mit dem das Ablaßventil HV 03 betätigt wird (enthält auch Ausfall des Druckknopfes), versagt,
- das Ablaßventil HV 03 nicht von Hand vor Ort geöffnet wird,
- das Ablaßventil HV 03 sich nicht öffnen läßt (weder von Hand noch durch Ablassen der Druckluft).

6.2.2.9 Fehlerbaum 11:
Explosion im Kocher (Bild 6.14)

Zu einer Explosion im Kocher kann es kommen, wenn folgende Systeme ausfallen, ohne daß Gegenmaßnahmen ergriffen werden:

- Kühlung des Kochers,
- Gasabzugsystem,
- Rührer.

Als Ausfallursachen, die zum Versagen der Kühlung des Kochers führen, sind möglich:

- Ausfall des Wasserkühlkreislaufes (Übertrag aus Fehlerbaum 8);
- Ausfall der Temperaturmessung TE 17 oder Ausfall des nachgeschalteten Meßumformers TY 17 in der Weise, daß die Temperatur unterhalb des Grenzwertes zu liegen scheint, obwohl sie in Wirklichkeit oberhalb liegt (beide sind dem Temperaturalarm TAH 17 und dem Kühlungsregler TIC 17 vorgeschaltet und führen somit zum Ausfall der Kühlung, da die automatische Regelung versagt und die Notwendigkeit von Handmaßnahmen nicht erkannt werden kann);
- Ausfall der automatischen Temperaturregelung durch Ausfall des Reglers TIC 17 mit zu geringem Durchsatz oder Ausfall des Regelventils TV 17 mit zu geringem Durchsatz, wenn gleichzeitig die manuelle Temperaturregelung, die ebenfalls eine ausreichende Kühlung erlaubt, nicht zum Ausgleich herangezogen wird. Dies kann der Fall sein, wenn das Handventil HV 13 mechanisch versagt oder der Temperaturalarm TAH 17 ausfällt. Im letztgenanntem Falle weiß der Operateur

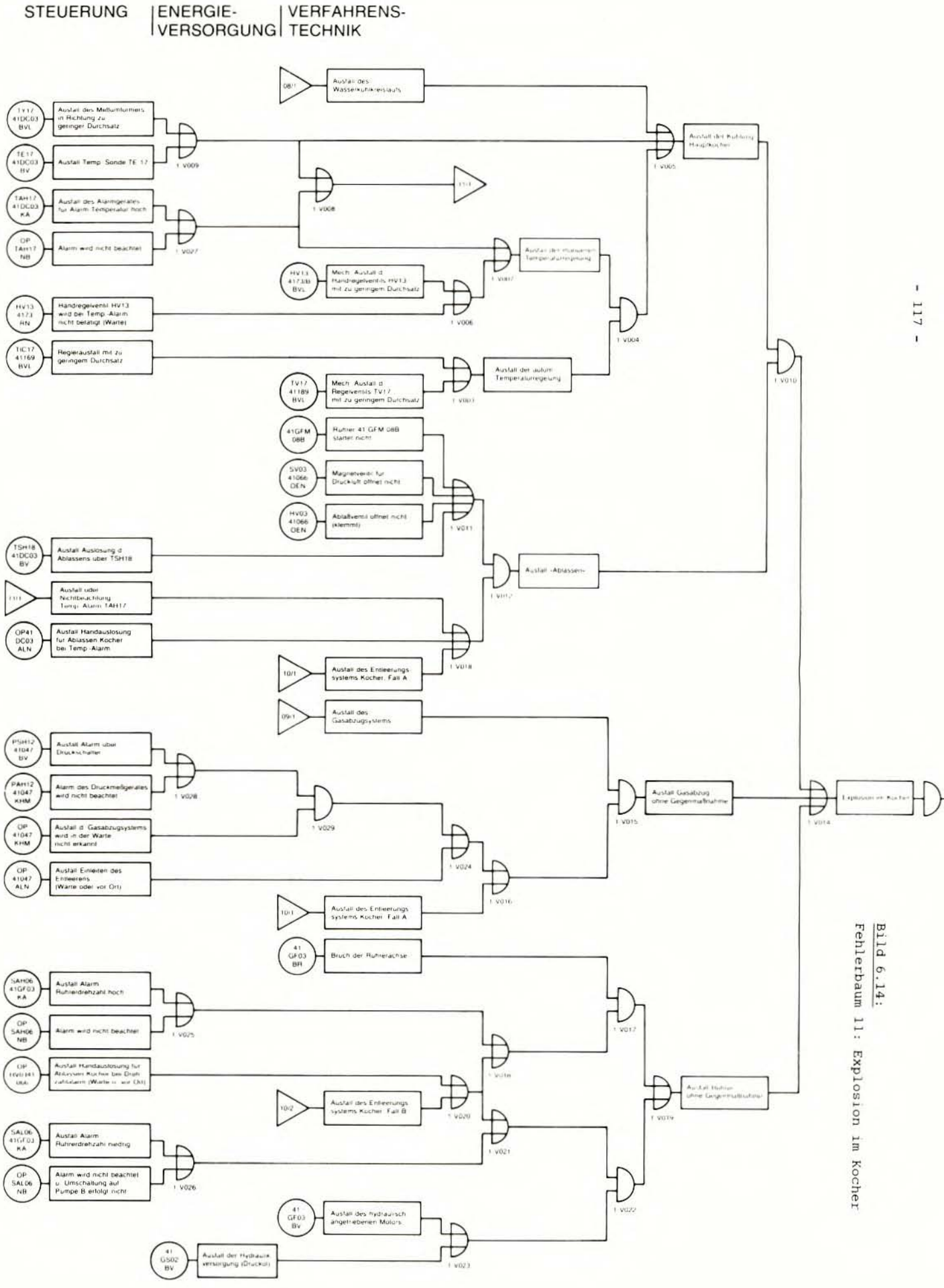


Bild 6.14:
Fehlerbaum 11: Explosion im Kocher

nicht, daß die Reaktionstemperatur ansteigt und die Kühlung verstärkt werden müßte.

Zur Vermeidung einer Explosion im Kocher bei Kühlungsausfällen bleibt lediglich das Ablassen des Inhalts in den Notablaßtank. Eine Explosion ereignet sich nur dann, wenn auch das Ablassen versagt. Dies könnte sein, wenn

- das Magnetventil SV 03 (öffnet nicht) oder das Ablaßventil HV 03 versagt, oder die automatische Auslösung durch Temperaturschalter TSH 18 ausfällt;
- das Handablassen ausfällt, da entweder wegen eines Ausfalls des Temperaturalarms TAH 17 oder der zugrundeliegenden Temperaturmessung TE 17 bzw. der Meßumformer TY 17 die Temperaturerhöhung nicht bemerkt und deshalb keine Maßnahme eingeleitet wird, der Alarm nicht beachtet oder die Handauslösung nicht betätgt wird oder das Notablassen des Kochers ausfällt (Übertrag 10/1 aus Fehlerbaum 10).

Zum Ausfall des Gasabzuges ohne entsprechende Gegenmaßnahmen zur Vermeidung einer Explosion kann es kommen, wenn

- das Gasabzugsystem ausfällt (Übertrag aus Fehlerbaum 9);
- der Ausfall des Gasabzugsystems nicht erkannt wird, weil die Farbfernsehkamera zur Überwachung der Farbe der Abgase und der Alarm PAH 12 ausgefallen sind oder keines der Signale beachtet wird, oder trotz erkannten Ausfalls die Entleerung des Kochers nicht rechtzeitig eingeleitet wird;
- das Entleerungssystem versagt (Übertrag 10/1 aus Fehlerbaum 10).

Ein Ausfall des Rührers "10" ohne Gegenmaßnahmen kann sich aus folgenden Ursachen ereignen:

- Bruch der Rührerachse,
- Ausfall des Alarms bei zu hoher Rührerdrehzahl, Nichtauslösen des Ablassens bei "Alarm Drehzahl hoch" oder Ausfall des Entleerungssystems des Kochers (Übertrag 10/2 aus Fehlerbaum 10),

- Ausfall des Hydraulikmotors oder Ausfall der Ölhydraulik (eigenes Hydrauliksystem für Kocher) und
- Ausfall des Alarms bei zu niedriger Rührerdrehzahl, Ausfall der Handauslösung bei Rühreralarm oder Ausfall des Entleerungssystems des Kochers (Übertrag 10/2 aus Fehlerbaum 10).

6.2.2.10 Fehlerbaum 12:
Ausfall des hydraulischen Transportsystems
(Bild 6.15)

Nach dem Abtrennen des Hexogens aus der Hexogen/Säure-Suspension über einen Drehfilter wird das Produkt durch ein hydraulisches Transportsystem zur Stabilisierung in ein anderes Gebäude gefördert (Bild 6.3). Das unerwünschte Ereignis bei diesem System ist der Ausfall der Förderung, der wie folgt eintreten kann:

- Ausfall beider Förderpumpen 42GA-03A/B für Umlaufwasser,
- Ausfall beider Förderpumpen 42GA-02A/B für die Rückförderung zum Transportwassertank "5",
- Ausfall des Niveauschalters LSLH 09 im Aufgabetrichter "1",
- Ausfall des vom Niveauschalter angesteuerten Motorventils SV 08,
- Bruch der Förderleitung,
- Verstopfen der Förderleitung,
- Ausfall des Regel- und Bypassventils in der Rückführleitung zum Transportwassertank "5",
- Ausfall des 3-Wege-Ventils in der Zufuhrleitung zu den Stabilisierungsreaktoren (die zur Abtrennung des Förderwassers dienende Nutsche wird ca. alle 6 h von Hand gekippt und in den Stabilisierungsreaktor entleert; vor dieser Maßnahme muß mit Hilfe des 3-Wege-Ventils auf den anderen Stabilisierungsreaktor umgeschaltet werden).

Der Ausfall der Förderpumpen 42GA-03A/B und 42GA-02A/B ist nach den gleichen Mechanismen möglich, wie eingangs beschrieben, so daß hier nur auf die Anregung der Umschaltung von der Betriebs- auf die Reservepumpe eingegangen wird.

Die Notwendigkeit einer Umschaltung nach Ausfall der Betriebspumpe wird durch die Alarme FAL 01A und FAL 01B (Alarme in den Warten von Nitrierer und Stabilisierung) in der Förderwasserzuleitung gemeldet. Das Umschalten auf die Reservepumpe kann infolgedessen dann nicht gelingen, wenn FAL 01A und FAL 01B ausfallen (zusammengefaßt zu einer Komponente im Fehlerbaum), beide Alarme nicht beachtet werden oder nicht umgeschaltet wird. (Nichtbeachten der Alarme und Unterlassen der Umschaltung sind zu einem Primärereignis zusammengefaßt.) Das Umschalten auf die Reservepumpe 42GA-02B erfolgt aufgrund des Niveaualarms LAH der Niveaumessung im Separiergefäß "6", so daß dessen Ausfall oder der des Startens der Reservepumpe auch bei Alarm (Alarm wird nicht beachtet oder Pumpe wird nicht gestartet) zum Ausfall des Transportsystems führt.

Über den Niveauschalter LSLH 09 und das Motorventil SV 08 wird der Füllstand im Aufgabetrichter geregelt. Der Niveauschalter LSLH 09 ist ein kapazitiver Niveaumesser, der bei einem eingestellten Grenzwert in beide Richtungen schaltet. Bei ansteigendem Niveau wird das Motorventil SV 08, über das der Bypassstrom zum Aufschwemmen des Produktbreies (Hexogen) vom Filter gesteuert wird, geöffnet, bei sinkendem Niveau geschlossen. Fällt eine der beiden Komponenten aus, ist die Produktförderung mit dem hydraulischen Transportsystem nicht mehr möglich.

Der Förderkreislauf kann durch Verstopfen ausfallen, wenn der im Separiergefäß "6" sich absetzende Feststoff nicht entleert wird. Dies ist in periodischen Abständen erforderlich. Erfolgt die Entleerung nicht, ist die Rückführung zum Transportwassertank unterbrochen, was den Ausfall des hydraulischen Transportsystems hervorruft.

Die Regelung der Rückführung des Wassers in den Transportwassertank "5" versagt, wenn

- das Regelventil LV 03 in geschlossenem Zustand ausfällt, der Ablaufregler LC 03 bei "Niveau hoch" im Separiergefäß keinen Öffnungsbefehl gibt oder die Druckluftversorgung des Regelventils ausfällt, da dieses so geschaltet ist, daß es

bei Druckluftausfall schließt (Beim allgemeinen Druckluftausfall ist dies jedoch unerheblich, da in diesem Fall alle Nitrierer und Kocher automatisch in die Notablaßbehälter abgelassen werden, so daß kein Produkt mehr anfällt. Zu einem relevanten Versagen führt folglich nur ein örtlicher Druckabfall der Druckluft.);

- das parallel zum Regelventil liegende Bypassventil, das die Förderung vom Separiergefäß "6" in den Transportwassertank "5" erlaubt, nicht geöffnet wird. Dies könnte sich ereignen, wenn der Niveaualarm des Separiergefäßes ausfällt oder das manuelle Bypassventil trotz Niveaualarm nicht geöffnet wird (Alarm wird nicht beachtet oder die erforderliche Maßnahme des Ventilöffnens wird nicht durchgeführt). Der Niveaualarm kann mehrere Ursachen haben, z.B. Pumpenausfall, so daß das Öffnen des Bypassventils nicht notwendigerweise die Reaktion auf den Niveaualarm sein muß. Das Öffnen des Bypassventils ME2-6 kann außerdem unmöglich sein, wenn es zum Beispiel klemmt.

Das periodisch umzuschaltende 3-Wege-Ventil, mit dem der Produktstrom jeweils einem der beiden Stabilisierungsreaktoren zugeführt wird, kann ausfallen und somit die weitere Förderung blockieren, indem

- das Ventil klemmt,
- die automatische Umschaltung durch die Wägeeinrichtung an der Nutsche versagt,
- bei Ausfall der automatischen Umschaltung eine Umschaltung von Hand nicht erfolgt. (Es ist dem Operateur bekannt, daß eine Umschaltung etwa alle 6 Stunden zu erfolgen hat, wobei auch die Nutsche in den Reaktor entleert werden muß.) Darüber hinaus erfolgt bei Überschreiten des Gewichtsgrenzwertes in der Nutsche ein Alarm über WAH 02A. (Das entsprechende Primärereignis enthält bereits den Ausfall dieses Alarms.)

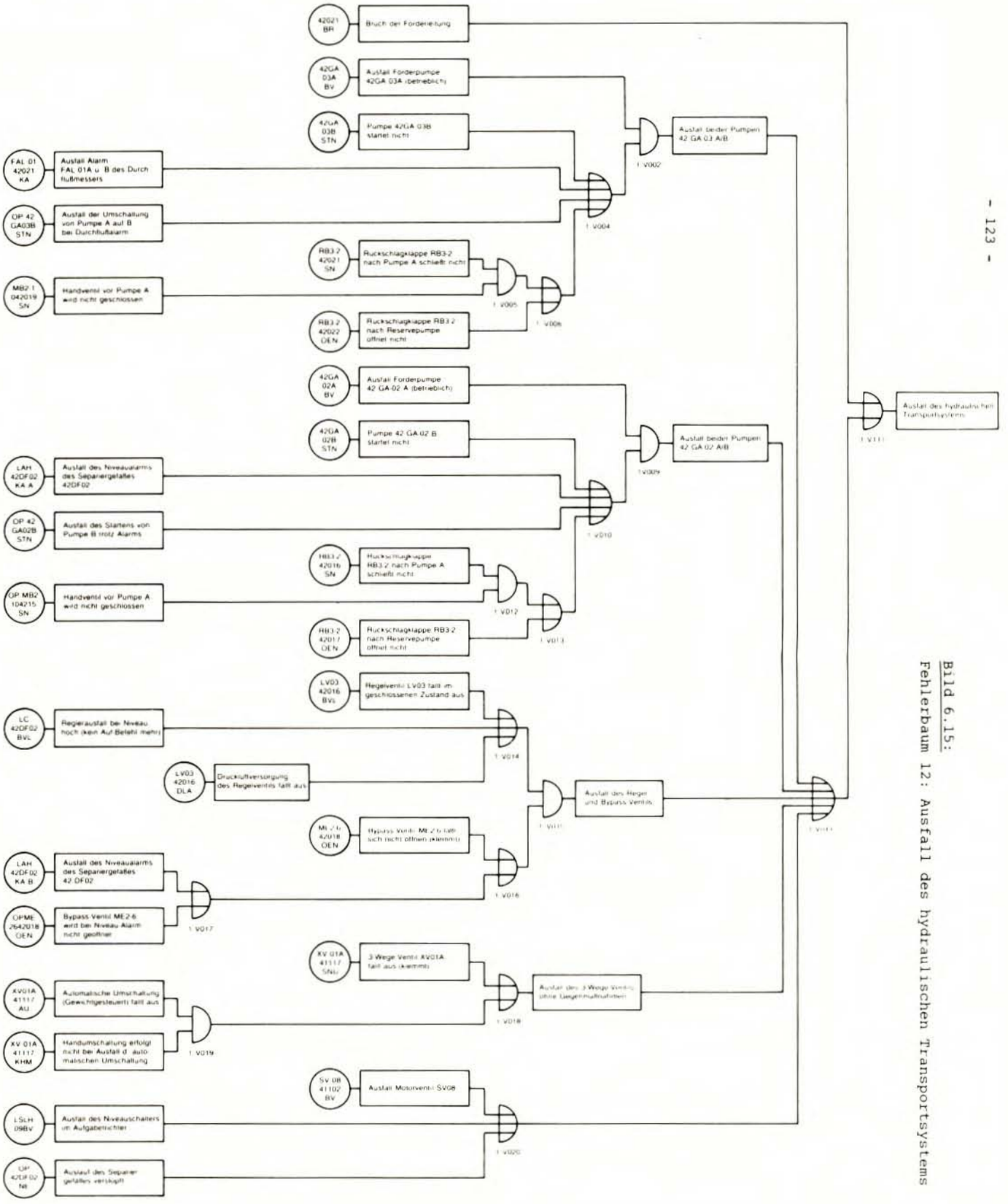


Bild 6.15:
Fehlerbaum 12: Ausfall des hydraulischen Transportsystems

6.2.3 Qualitative Ergebnisse der Fehlerbaumerstellung

Wie bereits in Kapitel 4 erwähnt, erfordert die Erstellung von Fehlerbäumen ein systematisches Aufsuchen von Komponentenausfällen, die allein oder gemeinsam mit dem Ausfall anderer Komponenten zum unerwünschten Ereignis führen. Dabei werden in der Regel bereits Schwachstellen im untersuchten System aufgedeckt, ohne daß schon eine Quantifizierung der Fehlerbäume durchgeführt worden wäre.

Bei der Erstellung der in den vorangehenden Abschnitten behandelten Fehlerbäume kam es ebenfalls zu einigen Verbesserungsvorschlägen, die dann bei der Anlagenerstellung berücksichtigt wurden. Sie sind zum Teil bereits in die Fehlerbäume eingearbeitet und werden nachfolgend im einzelnen behandelt.

- Fehlerbaum 1

Bei der Beurteilung der Frage, ob Kühlmittel in ausreichender Menge für die Kühlung des Nitrierers zur Verfügung steht, ist es wesentlich, die Vorlagemengen im Kühlmitteltank (warmer und kalter Teil) zu kennen. Sicherheitstechnisch bedeutsamer ist dabei die Vorlage im kalten Teil, da sich ein Ausfall hier direkt auf die Kühlung des Nitrierers auswirkt. Ursprünglich war lediglich eine lokale Niveauüberwachung des Kühlmitteltanks durch Schaugläser vorgesehen. Im Zuge der Fehlerbaumerstellung wurde als Systemänderung vom Anlagenhersteller ein "Niveau-Alarm niedrig" im warmen Teil des Kühlmitteltanks installiert. Dadurch läßt sich das Niveau aus der Warte überwachen und feststellen, ob ein zu geringer Durchfluß, der vom Meßinstrument FAL 01 gemeldet wird, auf Kühlmittelmangel im Tank zurückzuführen ist.

Ein Niveaualarm bei niedrigem Füllstand im kalten Teil des Kühlmitteltanks wäre aufgrund der qualitativen Analyse wünschenswert, da die Verfügbarkeit des Kühlmittels durch ihn erhöht würde.

Die Temperatur des Kühlmittels ist eine wichtige Einflußgröße für die Kühlung des Nitrierers. Sie sollte ursprünglich nur über Anzeigen in der Warte (eine Meßstelle im Strang vor dem kalten Teil des Kühlmitteltanks und eine Meßstelle im Zulauf zum Nitrierer) kontrolliert werden. Anzeigen, die nicht mit einem Alarm ausgerüstet sind, können nur dann die Einleitung von Gegenmaßnahmen hervorrufen, wenn das Überschreiten eines Grenzwertes bemerkt wird, was allerdings sehr unwahrscheinlich ist. Es wurde deshalb angeregt, eines der Instrumente mit einem Alarm zu versehen. Dies erfolgte beim Meßinstrument im Zulauf zum Nitrierer (TAH 04). Ausfälle in der Rückkühlung (auslösende Ereignisse N3.1/N3.2, Tabelle 6.4) können dadurch rechtzeitig erkannt werden, und es bleibt mehr Zeit für Gegenmaßnahmen. Zum Beispiel kann bei rechtzeitigem Erkennen des Temperaturanstieges die Hexaminzufuhr abgeschaltet werden, wodurch möglicherweise ein Ablassen des Nitriererinhaltes und somit ein Verlust des Nitriergutes vermieden werden kann.

In der ursprünglichen Auslegung hingegen würden Ausfälle in der Rückkühlung ein Ablassen des Reaktorinhaltes in den Notablaßtank erfordern, da sie erst durch Ansprechen des Alarms TAH 07A bzw. Ablassen des Nitriergutes in den Notablaßtank über TSHH 08A bemerkt würden.

- Fehlerbaum 3

Bei Ausfall der Kühlungsregelung des Nitrierers kann als Gegenmaßnahme von Hand ein Bypassventil geöffnet werden. Im Normalbetrieb ist dies geschlossen. Um bei Ausfällen des Regelventiles bzw. Reglers (auslösende Ereignisse N2.1, N2.2 in Tabelle 6.4) mehr Zeit für Gegenmaßnahmen zur Verfügung zu haben, wurde vorgeschlagen, mit der automatischen Durchflußregelung nur einen geringen Teilstrom des Kühlmittels zu regeln und den Rest über den teilweise geöffneten Bypass einzuspeisen, weil dann die Temperatur im Nitrierer langsamer ansteige.

Vom Anlagenhersteller wurde dies in Erwägung gezogen, jedoch noch nicht endgültig als Änderung aufgenommen, so daß in der Analyse davon ausgegangen wird, daß der Bypass normalerweise geschlossen ist.

- Fehlerbaum 8

Die Temperatur des Kühlwassers ist eine wichtige Einflußgröße für die Kühlung der Kocher. Ursprünglich sollte sie nur über eine Anzeige in der Warte (TI 05) kontrolliert werden. Wie beim Nitrierer wurde angeregt, die Temperaturmeßstelle zur Sicherstellung des Erkennens von Temperaturüberschreitungen mit einem Alarm zu versehen.

Vom Anlagenhersteller wurde dies als Änderung aufgenommen. Da jedoch für einen Temperturanstieg im Kühlsystem für den Kocher keine speziellen Gegenmaßnahmen spezifiziert und nur Provisorien möglich sind, ist damit noch keine Systemverbesserung verbunden.

- Fehlerbaum 9

Die Ableitung der Abgase aus den Kochern ist von besonderer sicherheitstechnischer Bedeutung. Ursprünglich war nur bei Ausfall eines Ventilators durch Motorschaden ein automatisches Umschalten auf den Reserveventilator vorgesehen. Während der Fehlerbaumerstellung wurde deshalb eine Systemänderung erarbeitet, durch die auch bei anderen Störungen im Gasabzugssystem, wie beispielsweise Verstopfungen oder Keilriemenriß, automatisch reagiert wird. An der schon vorhandenen Druckmeßstelle PI 12 wurde der Druckschalter PSH 12 installiert, über den bei Druckanstieg in der Gasabzugsleitung automatisch ein Motorventil geöffnet wird, durch das die Gase direkt im Naturzug an die Umgebung abgegeben werden.

- Fehlerbaum 12

In der ursprünglichen Version des hydraulischen Transportsystems wäre eine Störung in der Ablaufregelung des Separiergefäßes (T1.1-T1.3 in Tabelle 6.6) erst durch einen Niveaualarm im Transportwasserbehälter entdeckt worden. Wegen des im Vergleich zum Transportwasserbehälter (nutzbar 5 m^3, insgesamt 6 m^3) sehr geringen Volumens des Separiergefäßes (0,7 m^3 nutzbar, 1,3 m^3 insgesamt) wirken sich jedoch Durchsatzstörungen im Separiergefäß wesentlich stärker aus, so daß dieses schon voll ist bzw. überläuft, bevor der Niveaualarm im Transportwasserbehälter anspricht. Für Gegenmaßnahmen bleibt dann keine Zeit mehr. Das System muß abgeschaltet werden. Während der Fehlerbaumerstellung wurde deshalb angeregt, einen Niveaualarm im Separiergefäß zu installieren. Der Anlagenhersteller hat diese Änderung sofort gebilligt, so daß sie bei der Analyse schon berücksichtigt werden konnte. Bei den oben genannten Ausfällen bleibt jetzt für Gegenmaßnahmen ausreichend Zeit.

- Allgemeine Vorschläge

Im Zuge der Fehlerbaumerstellung konnten noch einige Schwachstellen in den Systemen aufgezeigt und durch Systemänderungen beseitigt werden. Darüber hinaus wurden noch Änderungen zur Beseitigung weiterer Schwachstellen empfohlen. Im einzelnen handelte es sich um folgende Vorschläge:

- Bei Druckluftausfall wird der Inhalt der Nitrierer automatisch in die Notablaßbehälter abgelassen ("fail safe"-Prinzip der Ablaßventile). Nach der ursprünglichen Auslegung würden in diesem Fall Säure und Hexamin weiter in den Reaktor strömen. Dies ist unerwünscht, da in einem solchen Falle nicht definierte Zustände im Reaktor auftreten können. Aufgrund der Überlegungen bei der Fehlerbaumerstellung wird das System so abgeändert, daß automatisch bei Druckluftausfall auch die Hexaminzufuhr und die Säureeinspeisung gestoppt werden.

- Zur Vermeidung von Folgeausfällen im zweiten Nitrierer bei Ausfall des ersten Nitrierers (Ablassen wegen zu hoher Temperatur) wird empfohlen, die Temperaturmeßstelle im zweiten Nitrierer in die Nähe der Eintrittsstelle des Nitriergutes aus dem ersten Nitrierer zu legen. Die Temperaturerhöhung würde dann im zweiten Nitrierer sicherer und schneller detektiert.
- Um sicherzustellen, daß beim Ablassen des Nitrierers die Hexaminzufuhr gestoppt wird, sollte beim Öffnen der Ablaßventile noch einmal ein Kontrollimpuls zum Stoppen der Hexaminzufuhr gegeben werden.
- Die Ventilatoren des Gasabzugsystems der Kocher waren ursprünglich so angeordnet, daß das Ausblasrohr am Reserveventilator durch Kondensat blockiert werden konnte. Aufgrund der Überlegungen bei der Fehlerbaumerstellung wurde die Anordnung der Gebläse so geändert, daß dies nicht mehr eintreten kann.
- Ursprünglich war vorgesehen, daß durch den Niveauschalter im Aufgabetrichter für Nitriergut des hydraulischen Transportsystems die Transportwasserförderpumpen abgeschaltet und von Hand wieder zugeschaltet werden. Da diese Steuerung zu störanfällig ist, wird sie jetzt so geändert, daß die Pumpen nicht mehr abgeschaltet werden. Durch den Niveauschalter wird jetzt nur mehr ein Motorventil betätigt, über das der Bypassstrom durch den Aufgabetrichter zum Aufschwemmen des Produktbreies eingestellt wird.

6.3 Zuverlässigkeitsdaten

6.3.1 Allgemeines

Nachdem in Kapitel 5 die allgemeinen Überlegungen bei der Ermittlung von Zuverlässigkeitsdaten dargelegt wurden, wird nachfolgend die Erstellung der speziellen Datenbasis für die Anlagenanalyse beschrieben. Die Auswahl von Ausfallraten für Komponenten erfolgte dabei hauptsächlich auf der Grundlage

der von der GRS in nuklearen und konventionellen Kraftwerken durchgeführten Erhebungen. Bei diesen sind im Gegensatz zu den ebenfalls herangezogenen Veröffentlichungen über Ausfallraten in Chemieanlagen Informationen über den Komponententyp und seine Einsatzbedingungen vorhanden. Deshalb wurden den eigenen Auswertungen - soweit sinnvoll - Angaben aus der Literatur vorgezogen. Bei der Bereitstellung der Daten wurden im wesentlichen fünf Anlagenbereiche unterschieden:

- Kühlkreisläufe für Nitrierer und Kocher,
- Nitrierer,
- Kocher,
- Gasabzug des Kochers,
- Förderung zwischen Nitrierung und Stabilisierung.

In jedem der genannten Bereiche gibt es Komponenten, die mit dem jeweiligen Betriebsmedium in Berührung stehen, und solche, die keinen Medienkontakt haben oder Druckluft als Arbeitsmedium benutzen.

Bei denjenigen Komponenten, die nicht mit einem Medium in Kontakt stehen, wurde normalerweise von einer Übertragbarkeit der Zuverlässigkeitsdaten aus dem Kraftwerksbereich auf die betrachtete Anlage ausgegangen. Dies erfolgte auch bei den Komponenten der Kühlkreisläufe, die im Falle der Kocherkühlung nur mit Wasser und bei der Nitriererkühlung mit einer Mischung von Wasser und 25 % Methanol beaufschlagt werden. Dabei wurde die Kühlmittelmischung in ihren Auswirkungen auf die Komponenten dem Wasser gleichgesetzt.

Die Daten für diejenigen Komponenten des Nitrierers, die Medienkontakt haben, stammen zum Teil aus eigenen Auswertungen für säurebeaufschlagte Komponenten. Darüber hinaus wurden Ausfallraten für Komponenten herangezogen, die mit Wasser beaufschlagt sind, und mit dem Medienbelastungsfaktor 2 oder 4 multipliziert, um die höhere Aggressivität der im Nitrierer und Kocher vorhandenen Stoffe zu berücksichtigen. Die gewählten Faktoren entsprechen denen, die in /6-6/ für Chemieanlagen

zur Herstellung organischer Stoffe und Säuren ermittelt worden sind. Es ist offensichtlich, daß eine solche Vorgehensweise nur ein Behelf sein kann, solange keine geeigneten Auswertungen für die betreffenden Komponenten und ihre spezifische Betriebssituation verfügbar sind. Für das Fördersystem zwischen Nitrierung und Stabilisierung wurden im wesentlichen Daten für wasserbeaufschlagte Komponenten verwendet. Der Einfluß von Flüssig-Feststoffgemischen auf die Ausfallraten wurde durch einen Medienbelastungsfaktor 2 abgeschätzt. Bei einigen Komponenten war es notwendig, Ausfallraten zu schätzen, da keine eigenen Beobachtungen vorlagen und auch nicht auf geeignete Literaturwerte zurückgegriffen werden konnte.

Einige Hilfssysteme, die nicht Gegenstand der vorliegenden Analyse sind, deren Versagen aber auf die betrachteten Anlagenteile Einfluß hat, wurden global bewertet. Dabei wurden Ausfallraten benutzt, wie sie bei vergleichbaren Anlagen in Kraftwerken beobachtet wurden. Die Wahrscheinlichkeiten für menschliches Fehlverhalten wurden auf der Grundlage der Werte und Bewertungsmethoden in /6-7/ ermittelt. Da die Anlage erst in Kürze in Betrieb gehen wird, sind noch nicht alle geplanten menschlichen Eingriffe bis in sämtliche Einzelheiten vorgeschrieben, so daß bei der Bewertung der Situationen, in denen der Mensch eingreifen muß, einige Festlegungen getroffen werden mußten. Diese könnten als Empfehlungen für das Betriebshandbuch aufgefaßt werden. Ungeplante menschliche Eingriffe wurden nicht berücksichtigt.

Im Abschnitt 6.3.2 werden die Ausfallraten für die einzelnen Komponenten aufgeführt und kommentiert. Die Zuordnung der einzelnen Werte zu den Primärereignissen der Fehlerbäume ist der Tabelle 6.7 zu entnehmen. Die Bewertung der menschlichen Eingriffe und die daraus sich ergebenden Versagenswahrscheinlichkeiten werden im Abschnitt 6.3.3 dargestellt. Ihre Zuordnung zu den Primärereignissen der Fehlerbäume erfolgt im Abschnitt 6.3.3.2.

Tab. 6.7:

Zuordnung der Ausfallraten für technische Komponenten zu den Primärereignissen der Fehlerbäume aus den Bildern 6.4 - 6.15

Fehlerbaum 1

Beschreibung des Ereignisses	Schlüssel	Betriebs- bzw. Umgebungsmedium	Median in $10^{-6}\ h^{-1}$	Mittelwert in $10^{-6}\ h^{-1}$	Streufaktor	Bemerkungen
Ausfall Alarm über Durchflußmesser FAL/01-40010	FAL 01 40010 KA	Kühlmittel	16	28	5,8	[1] [3]
Betriebsversagen Betriebspumpe 40GA-01A	40 GA-01 A BV	Kühlmittel	42	44	1,9	[*]
Rückschlagklappe RB2-1 hinter Betriebspumpe schließt nicht	RB2-1 40011 SN	Kühlmittel	0,28	0,5	6,0	Streufaktor geschätzt [2]
Rückschlagklappe RB2-1 hinter Reservepumpe öffnet nicht	RB2-1 40009 OEN	Kühlmittel	0,28	0,5	6,0	Streufaktor geschätzt [2]
Durch Leckage zu geringe Einspeisung in den kalten Kühlmitteltank	LE 40010-40001	Kühlmittel	1,4	2,5	6,0	Streufaktor geschätzt [*]
Ausfall des Rückkühlsystems	40 EA-01 BV	Frigen	168	210	3,0	Streufaktor geschätzt [*]
Ausfall Thermostatschalter für Rückkühlsystem	TS.40001 BV	Kühlmittel	3,2	3,6	2,2	[*]
Ausfall Temperaturalarm TI/04	TAHO 44001 KA	Kühlmittel	3,2	3,6	2,2	[1] [3]
Reservepumpe 40GA-01B startet nicht	OF 40 GA-01 B STN	Kühlmittel	11	13	3,2	[2]

[1]) Wartungsintervall τ = 672 h
[2]) Wartungsintervall τ = 168 h
[3]) Zusätzlich zum Komponentenausfall wird ein Kalibrierfehler mit $p_{50} = 10^{-2}/K = 5$ berücksichtigt.
[*]) Auslösendes Ereignis; unterscheidet sich der Schlüssel von Komponenten nur um den letzten Buchstaben, so handelt es sich um ein und dieselbe Komponente.

Tab. 6.7: (Fortsetzung)

Fehlerbaum 2

Beschreibung des Ereignisses	Schlüssel	Betriebs- bzw. Umgebungsmedium	Median in 10^{-6} h^{-1}	Mittelwert in 10^{-6} h^{-1}	Streufaktor	Bemerkungen
Unentdeckte Rohrleckage nach Druckschalter	Rohr L.N. DR SCH.	Kühlmittel	0,06	0,1	6	geschätzt[4])
Ausfall der Betriebspumpe 40-GA-02A	40 GA-02 A BV	Kühlmittel	42	44	1,9	[4])
Ausfall des Alarms über Druckschalter PSL 06	PAL 06 40004 KA B	Kühlmittel	6,5	9,5	4,2	[1]) [3])
Reservepumpe 40 GA 02B startet nicht	40 GA-02B STN	Kühlmittel	11	13	3,2	[2])
Rückschlagklappe RB2-1 hinter Reservepumpe öffnet nicht	RB2-1 40004 OEN	Kühlmittel	0,28	0,5	6	Streufaktor geschätzt[2])
Rückschlagklappe RB2-1 hinter 40-GA-02A schließt nicht	RB2-1 40005 SN	Kühlmittel	0,28	0,5	6	Streufaktor geschätzt[2])
Ausfall des Alarms über Druckschalter PSL 06	PAL 06 40004 KA A	Kühlmittel	6,5	9,5	4,2	[1]) [3])
Hexaminzufuhr schaltet nicht ab (Handauslösung)	41 KD 03A/B SNA	Atmosphäre	1,4	2,0	4	Streufaktor geschätzt[2])
Ausfall des Abschaltsignals vom Druckschalter PSL 07 zur Hexaminschnecke	PSL 07 40004 ST	Kühlmittel	6,5	9,5	4,2	[1]) [3])
Hexaminzufuhr schaltet nicht ab (automatisch angesteuert)	41 KD 03 A/B SNA	Atmosphäre	1,4	2,0	4,0	Streufaktor geschätzt[2])
Schaltglied I versagt	I-SCH GLIED	Atmosphäre	0,3	0,37	3	Θ = 8760 h

[1]) Wartungsintervall Θ = 672 h
[2]) Wartungsintervall Θ = 168 h
[3]) Zusätzlich zum Komponentenausfall wird ein Kalibrierfehler mit $p_{50} = 10^{-2}/K = 5$ berücksichtigt.
[4]) Auslösendes Ereignis; unterscheidet sich der Schlüssel von Komponenten nur um den letzten Buchstaben, so handelt es sich um ein und dieselbe Komponente.

Fehlerbaum 3

Beschreibung des Ereignisses	Schlüssel	Betriebs- bzw. Umgebungsmedium	Median in 10^{-6} h^{-1}	Mittelwert in 10^{-6} h^{-1}	Streufaktor	Bemerkungen
Mechanischer Ausfall des Regelventils TV 07A mit zu geringem Durchfluß	TV07 A41139 BV	Kühlmittel	21	29	3,6	[3])
Reglerausfall mit zu geringem Durchfluß	TICO 7A4139 BVL	Druckluft	43	44	1,5	[3])
Ausfall des Alarmgerätes für Alarm "Temperatur hoch"	TAHO 7A41EB 01AKA	Druckluft	6,5	9,5	4,2	[1]) [2])
Bypassventil läßt sich nicht öffnen	AB2-1 41139 OEN	Kühlmittel	0,2	0,25	3,2	[1])
Ausfall der Temperaturmessung	TE07 A4 1EB01 ABVL	Hexamin-Salpetersäure	1,9	3,5	6,0	Streufaktor geschätzt[3])
Ausfall pneumatischer Temperaturmeßumformer	TY7A 41EB01 ABVL	Atmosphäre	58	63	2	Streufaktor geschätzt[3])

[1]) Wartungsintervall Θ = 672 h
[2]) Zusätzlich zum Komponentenausfall wird ein Kalibrierfehler mit $p_{50} = 10^{-2}/K = 5$ berücksichtigt.
[3]) Auslösendes Ereignis; unterscheidet sich der Schlüssel von Komponenten nur um den letzten Buchstaben, so handelt es sich um ein und dieselbe Komponente.

Tab. 6.7: (Fortsetzung)

Fehlerbaum 4

Beschreibung des Ereignisses	Schlüssel	Betriebs- bzw. Umgebungsmedium	Median in 10^{-6} h^{-1}	Mittelwert in 10^{-6} h^{-1}	Streufaktor	Bemerkungen
Ausfall der Betriebspumpe 41-GA-01A	41 GA-01A BV	Salpetersäure	166	178	1,9	Werte entstehen durch Multiplikation der Werte für Wasser mit einem Umweltfaktor 4[4])
Reservepumpe 41-GA-01B startet nicht	41 GA-01B STN	Salpetersäure	42	54	3,2	[2])
Rückschlagklappe RB2-5 hinter Reservepumpe öffnet nicht	RB2-5 41001 OEN	Salpetersäure	1,1	2,0	6	Werte entstehen durch Multiplikation der Werte für Wasser mit einem Umweltfaktor 4[4])
Rückschlagklappe RB2-5 hinter Betriebspumpe schließt nicht	RB 2-5 41005 SN	Salpetersäure	1,1	2,0	6	[2])
Ausfall Niveaualarm niedrig im Vorlagebehälter	LAL 04 41 DF02 KA	Salpetersäure	18	20	2,2	[1])
Ausfall Alarm Durchfluß niedrig des 1.Rotameters	FADO1 A4 1007 KA	Salpetersäure	64	115	6	Streufaktor geschätzt[1])[3])
Ausfall des Abschaltbefehls für Hexamin vom Niveaumesser	LSIH 41 DF02 SNA	Salpetersäure	18	20	2,2	[1])
Schaltglied I versagt	I-SCH GLIED	Atmosphäre	0,3	0,37	3	θ = 8760 h
Hexaminzufuhr schaltet nicht ab (automatisch angesteuert)	41 KD 03 A/B SNA	Atmosphäre	1,4	2,0	4	Streufaktor geschätzt[2])
Kein Abschaltbefehl bei Ausfall Speisepumpe 41-GA-01A/B	41-GA 01A/B SNA	Atmosphäre	0,7	1,0	4	Streufaktor geschätzt[2])
Ausfall des 2. Rotameters	FSL02 A4 1007 SNA	Salpetersäure	64	115	6	Streufaktor geschätzt[2])[3])

[1]) Wartungsintervall θ = 672 h
[2]) Wartungsintervall θ = 168 h
[3]) Zusätzlich zum Komponentenausfall wird ein Kalibrierfehler mit $p_{50} = 10^{-2}/K = 5$ berücksichtigt.
[4]) Auslösendes Ereignis; unterscheidet sich der Schlüssel von Komponenten nur um den letzten Buchstaben, so handelt es sich um ein und dieselbe Komponente.

Tab. 6.7: (Fortsetzung)

Fehlerbaum 5

Beschreibung des Ereignisses	Schlüssel	Betriebs- bzw. Umgebungsmedium	Median in 10^{-6} h^{-1}	Mittelwert in 10^{-6} h^{-1}	Streu-faktor	Bemerkungen
Vorventil für Ablassen klemmt	SV01A 41026 OEN A	Atmosphäre	21	32	4,5	[2]
Ablaßventil klemmt (öffnet nicht)	HV01A 41026 OEN A	Salpetersäure + Hexamin	1,7	3	6	geschätzt[2]
Vorventil für Ablassen klemmt	SV01A 41026 OEN B	Atmosphäre	21	32	4,5	[2]
Ablaßventil klemmt (öffnet nicht)	HV01A 41026 OEN B	Salpetersäure + Hexamin	1,7	3	6	geschätzt[2]
Hexaminzufuhr schaltet nicht ab (Handauslösung)	41-KD 03A/B SNA	Atmosphäre	1,4	2,0	4	Streufaktor geschätzt[2]
Ausfall des Alarmgerätes für Alarm Temperatur hoch	TAH07A41EB 01 AKA	Atmosphäre/ Druckluft	6,5	9,5	4,2	[1][3]
Ausfall Grenzwertgeber niedrig	TSH 08ABV	Atmosphäre	8,4	12	4	Streufaktor geschätzt[1]
Rührer 41 GFM 08A startet nicht	41 GFM 08A A	Atmosphäre	4,3	5,4	3	Streufaktor geschätzt[1]
Rührer 41 GFM 08A startet nicht	41 GFM 08A B	Atmosphäre	4,3	5,4	3	Streufaktor geschätzt[1]
Rührer 41 GFM 08A startet nicht	41 GFM 08A C	Atmosphäre	4,3	5,4	3	Streufaktor geschätzt[1]
Ausfall Widerstandsthermometer TE08A niedrig	TE 08A BV	Salpetersäure + Hexamin	1,9	3,5	6,0	Streufaktor geschätzt[1]
Ausfall Grenzwertgeber niedrig	TSHH 08A ABV	Atmosphäre	8,4	12	4	[1][3]
Vorventil für Ablassen klemmt (öffnet nicht)	SV01A 41026 OEN C	Atmosphäre	21	32	4,5	[2]
Ablaßventil klemmt (öffnet nicht)	HV01A 41026 OEN C	Salpetersäure + Hexamin	1,7	3	6	geschätzt[2]

[1]) Wartungsintervall Θ = 672 h
[2]) Wartungsintervall Θ = 168 h
[3]) Zusätzlich zum Komponentenausfall wird ein Kalibrierfehler mit $p_{50} = 10^{-2}/K = 5$ berücksichtigt.

Fehlerbaum 6 und 7

Beschreibung des Ereignisses	Schlüssel	Betriebs- bzw. Umgebungsmedium	Median in 10^{-6} h^{-1}	Mittelwert in 10^{-6} h^{-1}	Streu-faktor	Bemerkungen
Plötzliche relativ große Leckage von Sole in den Nitrierreaktor	41 EB-01A LE	Salpetersäure + Hexamin	0,06	0,1	5	geschätzt[3]
Bruch der Rührerwelle von 41-GF-01A	41 GF-01A BR	Salpetersäure + Hexamin	0,08	0,2	10	geschätzt[3]
Ausfall Alarm Rührerdrehzahl hoch SAH/04A	SAH 04A41GF01 AKA	Atmosphäre	7,9	13	5	Streufaktor geschätzt [1][2]
Ausfall Alarm Rührerdrehzahl niedrig	SAL 04A41GF01 AKA	Atmosphäre	7,9	13	5	Streufaktor geschätzt [1][2]
Ausfall des hydraulisch angetriebenen Motors	41 GF-01A BV	Drucköl	0,38	1,0	10	geschätzt[3]
Ausfall der Hydraulikversorgung (Drucköl)	41-GS01 BV	Drucköl	3,0	8,0	10	geschätzt[3]

[1]) Wartungsintervall Θ = 672 h
[2]) Zusätzlich zum Komponentenausfall wird ein Kalibrierfehler mit $p_{50} = 10^{-2}/K = 5$ berücksichtigt.
[3]) Auslösendes Ereignis; unterscheidet sich der Schlüssel von Komponenten nur um den letzten Buchstaben, so handelt es sich um ein und dieselbe Komponente.

Tab. 6.7: (Fortsetzung)

Fehlerbaum 8

Beschreibung des Ereignisses	Schlüssel	Betriebs- bzw. Umgebungsmedium	Median in 10^{-6} h^{-1}	Mittelwert in 10^{-6} h^{-1}	Streufaktor	Bemerkungen
Ausfall des Motors für Kühlturmventilator	40 EG01 MOTBV	Atmosphäre	16	20	3	Streufaktor geschätzt[4])
Ausfall des Kühlturmventilators durch Keilriemenriß	40 EG01 VENBR	Atmosphäre	14	17	3	Streufaktor geschätzt[4])
Ausfall Temperaturschalter für Ventilatorsteuerung	TSLO 740EG01 BVL	Wasser	3,2	3,6	2,2	[4])
Ausfall Temperaturschalter niedrig für Heizungssteuerung	TSLL084 OEG01 BVL	Wasser	3,2	3,6	2,2	[4])
Ausfall des Temperaturmeßinstruments TI/05 im Zulauf zum Kocher	TI054022 BV	Wasser	3,2	3,6	2,2	[1])
Kaltwasserpumpe 40-GA-04B startet nicht	40 GA 04B STN	Wasser	11	14	3,2	[2])
Rückschlagklappe RB2-1 hinter Reservepumpe öffnet nicht	RB2-1 40022 OEN	Wasser	0,28	0,5	6	Streufaktor geschätzt[4])
Ausfall der betrieblichen Kaltwasserförderpumpe 04-GA-04A	40 GA 04A BV	Wasser	42	44	1,9	[4])
Leckage im Kühlwasserkreislauf größer als max. Einspeiserate	40018 40022 LE	Wasser	1,5	2,8	6,0	geschätzt[4])
Ausfall des schwimmergesteuerten Einspeiseventils	LCV02 40076 OEN	Wasser	118	190	5	geschätzt[4])
Kein Einspeisewasser verfügbar	40076 SV	Wasser	70,7	114	5	geschätzt[4])
Ausfall Alarmgerät des Druckmessers PAL/09 bei Druck niedrig	PAL 09 400022 KA	Wasser	6,5	9,5	4,2	[1]) [3])
Rückschlagklappe RB2-1 hinter 40-GA-04A schließt nicht	RB2-1 40021 SN	Wasser	0,28	0,5	6	Streufaktor geschätzt[2])

[1]) Wartungsintervall τ = 672 h
[2]) Wartungsintervall τ = 168 h
[3]) Zusätzlich zum Komponentenausfall wird ein Kalibrierfehler mit $p_{50} = 10^{-2}/K = 5$ berücksichtigt.
[4]) Auslösendes Ereignis; unterscheidet sich der Schlüssel von Komponenten nur um den letzten Buchstaben, so handelt es sich um ein und dieselbe Komponente.

Tab. 6.7: (Fortsetzung)

Fehlerbaum 9 und 10

Beschreibung des Ereignisses	Schlüssel	Betriebs- bzw. Umgebungsmedium	Median in 10^{-6} h^{-1}	Mittelwert in 10^{-6} h^{-1}	Streufaktor	Bemerkungen
Ausfall des Ventilatormotors 41-GD-M2 A	41 GDM2A BV	Atmosphäre	16	20	3	Streufaktor geschätzt*)
Keilriemenriß Ventilator A	41 GDO2A KR	Atmosphäre	14	17	3	Streufaktor geschätzt*)
Absorption ist blockiert	41 113 BL	Abgase	1,4	2,0	4	geschätzt*)
Ventilator 41-GD-M2 B startet nicht	41 GDM2B STN	Atmosphäre	3,6	4,5	3	Streufaktor geschätzt[2])
Ausfall der automatischen Umschaltung auf Ventilator B	AU 41GDM2B STN	Atmosphäre	2,1	3,0	4	Streufaktor geschätzt[2])
Ausfall Druckschalter incl. Alarm- und Abschaltsignal	PSH 12 41047 BV	Abgase	13	19	4,2	Mittelwert mit Medieneinflußfaktor 2 multipliziert[1])[3])
Motorventil für Ableitung klemmt (öffnet nicht)	41113 MV OEN	Abgase	13	16,0	3	[1])
Rührer 41 GFM 08B startet nicht	41 GFM 08B A	Atmosphäre	4,3	5,4	3	Streufaktor geschätzt[1])
Rührer 41 GFM 08B startet nicht	41 GFM 08B B	Atmosphäre	4,3	5,4	3	Streufaktor geschätzt[1])
Magnetventil für Druckluft öffnet nicht (klemmt)	SV 03 41066 OEN	Atmosphäre	21	32	4,5	[2])
Ablaßventil öffnet nicht (klemmt)	HV03 41066 OEN	Salpetersäure/ Hexamin/Hexogen	3,4	6	6	geschätzt, Wert für Nitrierreaktor mit Medieneinflußfaktor 2 multipliziert[2])

[1]) Wartungsintervall Θ = 672 h
[2]) Wartungsintervall Θ = 168 h
[3]) Zusätzlich zum Komponentenausfall wird ein Kalibrierfehler mit $p_{50} = 10^{-2}/K = 5$ berücksichtigt.
*) Auslösendes Ereignis; unterscheidet sich der Schlüssel von Komponenten nur um den letzten Buchstaben, so handelt es sich um ein und dieselbe Komponente.

Tab. 6.7: (Fortsetzung)

Fehlerbaum 11

Beschreibung des Ereignisses	Schlüssel	Betriebs- bzw. Umgebungsmedium	Median in 10^{-6} h^{-1}	Mittelwert in 10^{-6} h^{-1}	Streufaktor	Bemerkungen
Ausfall des Meßumformers in Richtung zu geringem Durchsatz	TY 17 41DC03 BVL	Atmosphäre/ Druckluft	57	63	2	Streufaktor geschätzt*)
Ausfall der Temperaturmessung TE 17 für Kühlungsregelung und Alarm	TE 17 41DC03 BV	Salpetersäure, Hexamin,Hexogen	3,8	7,0	6	Streufaktor geschätzt*), Medieneinflußfaktor 2 gegenüber dem Wert für das Nitrieren
Ausfall des Alarmgeräts für Alarm Temperatur hoch	TAH 17 41DC03 KA	Atmosphäre/ Druckluft	6,5	9,5	4,2	[1])[3])
Mechanischer Ausfall des Handregelventils HV 13 mit zu geringem Durchsatz	HV 13 4173 BVL	Wasser	9,8	12	3	[1])
Reglerausfall mit geringem Durchsatz	TIC 17 41169 BVL	Atmosphäre	42	44	1,3	*)
Mechanischer Ausfall des Regelventils TV 17 mit zu geringem Durchsatz	TV 17 41169 BVL	Wasser	21	29	1,6	*)
Magnetventil für Druckluft öffnet nicht	SV03 41066 OEN	Atmosphäre/ Druckluft	21	32	4,5	[2])
Ablaßventil öffnet nicht (klemmt)	HV03 41066 OEN	Hexamin,Hexogen, Salpetersäure	3,4	6	6	geschätzt[2]), Wert für Nitrierreaktor mit Medieneinflußfaktor 2 multipliziert
Ausfall der automatischen Auslösung (über Instrument TSH 18 Temperatur zu hoch)	TSH 18 41DC03 BV	Hexamin,Hexogen, Salpetersäure	7,7	14	6	Mittelwert mit Medieneinflußfaktor 4 multipliziert, Streufaktor geschätzt*)[3])
Ausfall Alarm über Druckschalter	PSH 12 41047 BV	Abgase	13	19	4,2	Mittelwert mit Umweltfaktor 2 multipliziert [1])[3])
Bruch der Rührerachse	41GF03 BR	Hexamin,Hexogen, Salpetersäure	0,15	0,4	10	Mittelwert mit Faktor 2 gegenüber Nitrierreaktor wegen hoher Temperatur multipliziert*)
Ausfall Alarm Rührerdrehzahl hoch	SAH 06 41GF03 KA	Atmosphäre	7,9	13	5	Streufaktor geschätzt*)[4])
Ausfall Alarm Rührerdrehzahl niedrig	SAL 06 41GF03 KA	Atmosphäre	7,9	13	5	Streufaktor geschätzt*)[4])
Ausfall des hydraulisch getriebenen Motors	41GF03 BV	Drucköl	0,38	1,0	10	geschätzt*)
Ausfall der Hydraulikversorgung Drucköl	41GS02 BV	Drucköl	3,0	8,0	10	[4])
Rührer 41 GFM 08B startet nicht	41 GFM 08 B	Atmosphäre	4,3	5,4	3	Streufaktor geschätzt[1])

[1]) Wartungsintervall τ = 672 h
[2]) Wartungsintervall τ = 168 h
[3]) Zusätzlich zum Komponentenausfall wird ein Kalibrierfehler mit $p_{50} = 10^{-2}/K = 5$ berücksichtigt.
[4]) Auslösendes Ereignis; unterscheidet sich der Schlüssel von Komponenten nur an den letzten Buchstaben, so handelt es sich um ein und dieselbe Komponente.

Tab. 6.7: (Fortsetzung)

Fehlerbaum 12

Beschreibung des Ereignisses	Schlüssel	Betriebs- bzw. Umgebungsmedium	Median in 10^{-6} h^{-1}	Mittelwert in 10^{-6} h^{-1}	Streufaktor	Bemerkungen
Ausfall Förderpumpe 42-GA 03A (betrieblich)	42 GA03A BV	Wasser	42	44	1,9	[4])
Pumpe 42 GA-03 B startet nicht	42 GA03B STN	Wasser	11	13	3,2	[2])
Ausfall Alarm des Durchflußmessers	FALO1 42021 KA	Wasser	16	28	5,8	[1])[3])
Rückschlagklappe RB3-2 hinter Pumpe A schließt nicht	RB3-2 42021 SN	Wasser	0,28	0,5	6	Streufaktor geschätzt[2])
Rückschlagklappe RB3-2 hinter Reservepumpe öffnet nicht	RB3-2 42022 OEN	Wasser	0,28	0,5	6	Streufaktor geschätzt[2])
Bruch der Förderleitung	42 021 BR	Wasser/Hexogen	0,06	0,1	6	geschätzt[4])
Ausfall der Förderpumpe 42 GA-02-A (betrieblich)	42 GA02A BV	Wasser/Hexogen	82	88	1,9	Wert für Wasser mit Medieneinflußfaktor 2 multipliziert[4])
Pumpe 42-GA-02B startet nicht	42 GA02B STN	Wasser/Hexogen	22	26	3,2	[2])
Ausfall des Niveaualarms des Separiergefäßes 42DF02	LAH 42DF02 KA A	Wasser/Hexogen	121	195	5	geschätzt [1])[3])
Rückschlagklappe RB3-2 hinter Pumpe A schließt nicht	RB3-2 42016 SN	Wasser/Hexogen	0,28	0,5	6	Streufaktor geschätzt[2])
Rückschlagklappe RB3-2 hinter Reservepumpe öffnet nicht	RB3-2 42017 OEN	Wasser/Hexogen	0,28	0,5	6	Streufaktor geschätzt[2])
Regelventil LV03 fällt im geschlossenen Zustand aus	LV03 42016 BVL	Wasser/Hexogen	42	57	3,6	[4])
Reglerausfall bei Niveau hoch	LC 42DF02 BVL	Wasser/Hexogen	121	195	5	geschätzt[4])
Druckluftversorgung des Regelventils fällt aus	LV03 42016 DLA	Atmosphäre	51	65	3	Streufaktor geschätzt[4])
Bypassventil ME2-6 läßt sich nicht öffnen (klemmt)	ME2-6 42018 OEN	Wasser/Hexogen	0,39	0,50	3,2	Werte für Wasser mit Medienbelastungsfaktor 2 multipliziert[1])
Ausfall des Niveaualarms des Separiergefäßes 42 DF 02	LAH 42DF02 KA B	Wasser/Hexogen	121	195	5	[1])[3])
Dreiwegeventil XV01A fällt aus (klemmt)	XV01A 41117 SNU	Wasser/Hexogen	62	100	5	geschätzt[4])
Automatische Umschaltung (gewichtgesteuert) fällt aus	XV01A 41117 AU	Atmosphäre	1,6	3,0	6	geschätzt[4])
Ausfall Motorventil SV 08	SV08 41102 BV	Wasser	12,8	16	3	[4])
Ausfall des Niveauschalters im Aufgabetrichter	LSLH 09 BV	Wasser/Hexogen	4,0	5,7	4	geschätzt[4])

[1]) Wartungsintervall Θ = 672 h
[2]) Wartungsintervall Θ = 168 h
[3]) Zusätzlich zum Komponentenausfall wird ein Kalibrierfehler mit $p_{50} = 10^{-2}/K = 5$ berücksichtigt.
[4]) Auslösendes Ereignis; unterscheidet sich der Schlüssel von Komponenten nur um den letzten Buchstaben, so handelt es sich um ein und dieselbe Komponente.

6.3.2 Ausfallraten für Komponenten und Betriebsmittel

6.3.2.1 Komponenten oder Betriebsmittel ohne Betriebsmedienkontakt oder mit Druckluft als Arbeitsmedium

- Ausfall eines Endschalters

  $\lambda = 2 \cdot 10^{-6}\ h^{-1}$ (Einzelwert, eigene Auswertung)
  K = 4 (geschätzt)

- Drehzahlmesser mit Alarm fällt hoch oder niedrig aus

  $\lambda = 12{,}7 \cdot 10^{-6}\ h^{-1}$ (Einzelwert, eigene Auswertung)
  K = 5 (geschätzt)

- Ausfall des Motors eines Ventilators

  $\lambda = 20 \cdot 10^{-6}\ h^{-1}$ (Einzelwert, eigene Auswertung)
  K = 3 (geschätzt)

- Keilriemenriß

  $\lambda = 17 \cdot 10^{-6}\ h^{-1}$ (Einzelwert, eigene Auswertung)
  K = 3 (geschätzt)

- Ausfall der automatischen Umschaltung eines Elektromotors auf einen Reservemotor

  $\lambda = 3{,}0 \cdot 10^{-6}\ h^{-1}$ (Einzelwert, eigene Auswertung)
  K = 4 (geschätzt)

- Ausfall eines I/P-Wandlers

  $\lambda = 62{,}8 \cdot 10^{-6}\ h^{-1}$
  K = 2 (geschätzt)

  Die Ausfallrate wurde aufgrund der Werte $61{,}6 \cdot 10^{-6}\ h^{-1}$ und $63{,}9 \cdot 10^{-6}\ h^{-1}$, die in /6-6/ für Werke zur Herstellung organischer Stoffe sowie organischer Stoffe und Säuren (Werk A bzw. B) angegeben werden, ermittelt. Eigene Auswertungen lagen für I/P-Wandler nicht vor. Um ein breites Spektrum von möglichen Belastungsarten zu berücksichtigen,

wurde K = 2 benutzt anstelle des Wertes K = 1,04, der sich aufgrund der nahe beieinanderliegenden Werte aus /6-6/ ergibt.

- Versagen eines elektrischen Druckknopfes

  $\lambda = 0{,}5 \cdot 10^{-6}\ h^{-1}$ /6-8/
  K = 3 (geschätzt)

- Motorschalter schaltet nicht ab

  $\lambda = 10^{-6}\ h^{-1}$ (Einzelwert, eigene Auswertung)
  K = 4 (geschätzt)

- Ausfall Grenzwertgeber für Temperaturmessung

  $\lambda = 12 \cdot 10^{-6}\ h^{-1}$ (Einzelwert, eigene Auswertung)
  K = 4 (geschätzt)

- Ausfall eines pneumatischen Temperaturalarms

  $\lambda = 9{,}5 \cdot 10^{-6}\ h^{-1}$
  K = 4,2
  Wert für Druckwächter gemäß eigener Auswertung

- Ausfall eines magnetischen Vorsteuerventils

  $\lambda = 31{,}7 \cdot 10^{-6}\ h^{-1}$
  K = 4,5

  Grundlage der Werte sind drei Ausfallraten aus eigenen Beobachtungen sowie die Werte $34{,}3 \cdot 10^{-6}\ h^{-1}$ und $87{,}2 \cdot 10^{-6}\ h^{-1}$, die in /6-6/ für Anlagen zur Herstellung organischer Stoffe bzw. organischer Stoffe und Säuren (Werk A und B) angegeben werden.

- Ausfall eines pneumatischen Reglers

  $\lambda = 43{,}6 \cdot 10^{-6}\ h^{-1}$
  K = 1,5

  Der Wert wurde aufgrund der folgenden Ausfallraten ermittelt: $42 \cdot 10^{-6}\ h^{-1}$, $43 \cdot 10^{-6}\ h^{-1}$, $58{,}8 \cdot 10^{-6}\ h^{-1}$,

$50,3 \cdot 10^{-6}\ h^{-1}$ für petrochemische Anlagen /6-9/ und $29,7 \cdot 10^{-6}\ h^{-1}$, $36,5 \cdot 10^{-6}\ h^{-1}$, die in /6-6/ für die Herstellung organischer Stoffe bzw. organischer Stoffe und Säuren (Werk A und B) angegeben werden. Eigene Auswertungen lagen nicht vor.

- ODER-Schaltglied mit 5 Eingängen versagt

  $\lambda = 0,37 \cdot 10^{-6}\ h^{-1}$

  $K = 3,0$ aus /6-10/

- Startversagen eines Elektromotors

  $\lambda = 5,4 \cdot 10^{-6}\ h^{-1}$ (Einzelwert, eigene Auswertung)

  $K = 3,0$ (geschätzt)

6.3.2.2 Mit Wasser oder Kühlmittel beaufschlagte Komponenten der Kühlkreisläufe

- Ausfall eines Durchflußmessers einschließlich Alarm

  $\lambda = 28,3 \cdot 10^{-6}\ h^{-1}$

  $K = 5,8$

  Der Wert beruht auf 6 Ausfallraten aus eigenen Beobachtungen.

- Betriebsversagen einer Pumpe einschließlich Ansteuerung

  $\lambda = 44,4 \cdot 10^{-6}\ h^{-1}$

  $K = 1,9$

  Der Wert beruht auf 6 Ausfallraten aus eigenen Beobachtungen.

- Startversagen einer Pumpe einschließlich Ansteuerung

  $\lambda = 13,4 \cdot 10^{-6}\ h^{-1}$

  $K = 3,2$

  Der Wert beruht auf 6 Ausfallraten aus eigenen Beobachtungen.

- Rückschlagklappe schließt bzw. öffnet nicht

  $\lambda = 0{,}5 \cdot 10^{-6}\ h^{-1}$ (Einzelwert, eigene Auswertung)

  $K = 6$ (geschätzt)

- Rohr- und Ventilleckagen

  Die Ausfallraten wurden auf der Grundlage von Daten aus eigenen Auswertungen für Rohr- bzw. Ventilleckagen unter Berücksichtigung der vorhandenen Anzahl von Ventilen und der Rohrlänge des zu beurteilenden Bereichs abgeschätzt.

- Ausfall Thermostatschalter oder Temperaturwächter einschließlich Alarm

  $\lambda = 3{,}6 \cdot 10^{-6}\ h^{-1}$

  $K = 2{,}2$

  Der Wert beruht auf 4 Ausfallraten aus eigenen Beobachtungen.

- Ausfall eines Druckwächters einschließlich Abschaltung oder Alarm

  $\lambda = 9{,}53 \cdot 10^{-6}\ h^{-1}$

  $K = 4{,}2$

  Der Wert beruht auf 10 Ausfallraten aus eigenen Beobachtungen.

- Pneumatisches Regelventil regelt nicht

  $\lambda = 28{,}7 \cdot 10^{-6}\ h^{-1}$

  $K = 3{,}6$

  Der Wert beruht auf 4 Ausfallraten aus eigenen Beobachtungen für elektrische Regelventile, die hier als Abschätzung dienen sollen.

- Handabsperrventil läßt sich nicht öffnen

  $\lambda = 0{,}25 \cdot 10^{-6}\ h^{-1}$

  $K = 3{,}2$

Der Wert beruht auf 4 Ausfallraten aus eigenen Beobachtungen.

- Ausfall eines schwimmergesteuerten Ventils

  $\lambda = 190 \cdot 10^{-6}\ h^{-1}$ (geschätzt)
  K = 5 (geschätzt)

- Handregelventil regelt nicht

  $\lambda = 12{,}3 \cdot 10^{-6}\ h^{-1}$ (Einzelwert, eigene Auswertung)
  K = 3 (geschätzt)

6.3.2.3 Komponenten, die im Bereich des Nitrierers mit Salpetersäure oder Einsatzstoffen und Produkten der Reaktion in Berührung kommen

- Ausfall Temperaturmessung mit Widerstandsthermometer

  $\lambda = 3{,}5 \cdot 10^{-6}\ h^{-1}$ (Einzelwert, eigene Auswertung)
  K = 6 (geschätzt)

  Die Ausfallrate stammt aus eigenen Auswertungen für ein Widerstandsthermometer in Schutzrohrausführung. Dies ist der Gerätetyp, der in der untersuchten Anlage verwendet wird. Die Ausfallrate, die in /6-6/ für ein Widerstandsthermometer bei Einsatz in einer Anlage zur Herstellung organischer Stoffe (Werk A) angegeben wird, beträgt $36{,}5 \cdot 10^{-6}\ h^{-1}$ und liegt somit erheblich über dem Wert der eigenen Auswertung. Dieser stimmt jedoch mit dem ebenfalls in /6-6/ angegebenen Wert für ein Quecksilberthermometer, das von einem Schutzrohr umgeben ist, überein. Aus Erfahrung ist bekannt, daß die Art des Schutzes des Temperaturfühlers wesentlichen Einfluß auf die Ausfallrate hat. Bei dem Wert für das Widerstandsthermometer aus /6-6/ handelt es sich offenbar um ein Gerät ohne Schutzrohr, das deshalb direkten Medienkontakt hat. Seine Ausfallrate dürfte mithin den vorliegenden Fall nicht zutreffend beschreiben.

- Betriebsausfall einer Pumpe für Salpetersäure

  $\lambda = 178 \cdot 10^{-6}\ h^{-1}$

  $K = 1,9$

  Die Ausfallrate wurde durch Multiplikation des Wertes für Wasserpumpen mit einem Medienbelastungsfaktor 4 ermittelt.

- Startausfall einer Pumpe für Salpetersäure

  $\lambda = 54 \cdot 10^{-6}\ h^{-1}$

  $K = 3,2$

  Die Ausfallrate wurde durch Multiplikation des Wertes für Wasserpumpen mit einem Medienbelastungsfaktor 4 ermittelt.

- Rückschlagklappe, die mit Salpetersäure beaufschlagt wird

  $\lambda = 2,0 \cdot 10^{-6}\ h^{-1}$

  $K = 6$

  Die Ausfallrate wurde durch Multiplikation des Wertes für das Medium Wasser mit einem Medienbelastungsfaktor 4 ermittelt.

- Ausfall eines kapazitiven Niveaumessers einschließlich Alarm- oder Abschaltsignal

  $\lambda = 20 \cdot 10^{-6}\ h^{-1}$

  $K = 2,2$

  Die Werte entstanden auf der Grundlage einer Ausfallrate aus eigenen Beobachtungen und der in /6-6/ für eine Fabrik zur Herstellung organischer Stoffe (Werk A) angegebenen Ausfallrate von $25,1 \cdot 10^{-6}\ h^{-1}$.

- Ausfall einer Durchflußmessung mit Rotameter

  $\lambda = 115 \cdot 10^{-6}\ h^{-1}$

  $K = 6$ (geschätzt)

  Die Ausfallrate wird in /6-6/ für eine Fabrik zur Herstellung organischer Stoffe (Werk A) angegeben.

- Absperrventil mit pneumatischem Antrieb öffnet nicht

  $\lambda = 3,0 \cdot 10^{-6}\ h^{-1}$ (Einzelwert, eigene Auswertung)
  $K = 6,0$ (geschätzt)

- Plötzliche relativ große Leckage von Kühlmittel in den Nitrierer

  $\lambda = 0,1 \cdot 10^{-6}\ h^{-1}$ (geschätzt)
  $K = 5$ (geschätzt)

- Bruch der Rührerwelle

  $\lambda = 0,2 \cdot 10^{-6}\ h^{-1}$ (geschätzt)
  $K = 10$ (geschätzt)

6.3.2.4 Komponenten, die im Kocher mit den Reaktionsprodukten in Berührung kommen

- Absperrventil mit pneumatischem Antrieb öffnet nicht

  $\lambda = 6,0 \cdot 10^{-6}\ h^{-1}$
  $K = 6,0$ (geschätzt)

  Die Ausfallrate ist durch Multiplikation des Wertes für den Nitrierer mit einem Medieneinflußfaktor 2 entstanden.

- Ausfall eines Temperaturschalters

  $\lambda = 14 \cdot 10^{-6}\ h^{-1}$
  $K = 6$ (geschätzt)

  Die Ausfallrate ist durch Multiplikation der für das Medium Wasser geltenden Werte mit einem Medieneinflußfaktor 4 berechnet worden.

- Bruch der Rührerachse

  $\lambda = 0,4 \cdot 10^{-6}\ h^{-1}$ (geschätzt)
  $K = 10$ (geschätzt)

Die Ausfallrate ist durch Multiplikation des Schätzwertes für den Nitrierer mit einem Medieneinflußfaktor 2 berechnet worden.

6.3.2.5 Gasabzug des Kochers

- Ausfall eines Druckwächters mit Schalter oder Alarm

  $\lambda = 19 \cdot 10^{-6}\ h^{-1}$

  $K = 4,2$

- Motorventil klemmt

  $\lambda = 16 \cdot 10^{-6}\ h^{-1}$ (Einzelwert, eigene Auswertung)

  $K = 3$ (geschätzt)

6.3.2.6 Fördersystem zwischen Nitrierung und Stabilisierung

- Betriebsausfall einer Pumpe

  $\lambda = 88 \cdot 10^{-6}\ h^{-1}$

  $K = 1,9$

  Die Ausfallrate wurde durch Multiplikation des beim Medium Wasser geltenden Wertes mit einem Medieneinflußfaktor 2 gewonnen.

- Startausfall einer Pumpe

  $\lambda = 26 \cdot 10^{-6}\ h^{-1}$

  $K = 3,2$

  Die Ausfallrate wurde durch Multiplikation des beim Medium Wasser geltenden Wertes mit einem Medieneinflußfaktor 2 gewonnen.

- Ausfall des Niveaualarms im Separiergefäß

  $\lambda = 195 \cdot 10^{-6}\ h^{-1}$ (geschätzt)

  $K = 5$ (geschätzt)

- Pneumatisches Regelventil öffnet nicht

  $\lambda = 57 \cdot 10^{-6}\ h^{-1}$

  $K = 3,6$

  Die Ausfallrate wurde durch Multiplikation des beim Medium Wasser geltenden Wertes mit dem Medieneinflußfaktor 2 gewonnen.

- Niveaureglerausfall

  $\lambda = 195 \cdot 10^{-6}\ h^{-1}$ (geschätzt)

  $K = 5$ (geschätzt)

- Handabsperrventil öffnet nicht

  $\lambda = 0,5 \cdot 10^{-6}\ h^{-1}$

  $K = 3,2$

  Die Ausfallrate wurde durch Multiplikation des beim Medium Wasser geltenden Wertes mit dem Medieneinflußfaktor 2 gewonnen.

- Dreiwegeventil schaltet nicht um

  $\lambda = 195 \cdot 10^{-6}\ h^{-1}$ (geschätzt)

  $K = 5$ (geschätzt)

- Gewichtgesteuerte Umschaltung versagt

  $\lambda = 3 \cdot 10^{-6}\ h^{-1}$ (geschätzt)

  $K = 6$ (geschätzt)

- Kapazitiver Niveaugeber versagt

  $\lambda = 5,7 \cdot 10^{-6}\ h^{-1}$ (Einzelwert, eigene Auswertung)

  $K = 4$ (geschätzt)

- Motorventil versagt

  $\lambda = 13,2 \cdot 10^{-6}\ h^{-1}$ (Einzelwert, eigene Auswertung)

  $K = 2$ (geschätzt)

6.3.2.7 Hilfssysteme

- Ausfall der Druckölversorgung

  $\lambda = 8 \cdot 10^{-6}\ h^{-1}$ (geschätzt)

  $K = 10$ (geschätzt)

- Ausfall eines Ölhydraulikmotors

  $\lambda = 10^{-6}\ h^{-1}$ (geschätzt)

  $K = 10$ (geschätzt)

- Ausfall der Druckluftversorgung

  $\lambda = 64 \cdot 10^{-6}\ h^{-1}$

  $K = 3$ (geschätzt)

  Die Ausfallrate beruht auf eigenen Erhebungen für in üblicher Weise ausgelegte Druckluftversorgungssysteme.

- Ausfall der Rückkühlung durch die Kältemaschine

  $\lambda = 210 \cdot 10^{-6}\ h^{-1}$

  $K = 3$ (geschätzt)

  Die Ausfallrate beruht auf eigenen Erhebungen für in üblicher Weise ausgelegte Rückkühlkreisläufe.

6.3.3 Bewertung menschlichen Fehlverhaltens

6.3.3.1 Vorbemerkung

Die nachfolgende Bewertung menschlichen Fehlverhaltens orientiert sich in Vorgehen und Daten an /6-7/.

Die genannte Arbeit hat zwar die Bewertung menschlicher Zuverlässigkeit im Bereich von Kernkraftwerken zum Gegenstand, die Vorgehensweise und weitgehend auch die Daten lassen sich aber nach unserer Meinung auf die Situation in der Prozeßindustrie übertragen. Es wird dabei nicht übersehen, daß unterschiedliche administrative Vorgaben, Organisationsformen, spezifische

Aufgaben oder Komponenten großen Einfluß auf Einzelfälle haben können. Derartige Einflußgrößen herauszufinden und entsprechend zu berücksichtigen, ist aber ohnehin eine Aufgabe der "Mensch/Maschine-System-Analyse". Darüber hinaus ist anzumerken, daß das in /6-7/ angegebene THERP-Verfahren (THERP = Technique for Human Error Rate Prediction) seit langem außerhalb der Kerntechnik benutzt wird und ursprünglich für Analysen militärischer Systeme entwickelt wurde. Die in /6-7/ angegebenen Daten beruhen neben subjektiven Abschätzungen auf einer Reihe von Untersuchungen und Auswertungen an militärischen Systemen, aus der Prozeßindustrie und aus Feldstudien. Im übrigen wird in /6-7/ ausgeführt, daß sich Arbeitsaufgaben in der chemischen Industrie und im Kraftwerksbereich sehr ähneln.

Im Rahmen der hier vorliegenden Untersuchung war es nicht möglich, eine detaillierte Analyse der Arbeitsaufgaben und -umstände in der Anlage durchzuführen. Aufgrund der somit fehlenden Detailangaben zu den ergonomisch relevanten Gesichtspunkten der Wartengestaltung, zu den Aspekten des Trainings, der Vorkenntnisse des Personals, zu organisatorischen und administrativen Randbedingungen sowie zu Arbeitshilfsmitteln (Prozeduren für Störungen) waren der Bewertung Beschränkungen auferlegt. Es wurde daher versucht, durch Erhöhung der in /6-7/ angegebenen Fehlerwahrscheinlichkeiten eine konservative Abschätzung vorzunehmen. Darüber hinaus wurde durch Erhöhung der Unsicherheitsfaktoren K die größere Unsicherheit bei der Bewertung berücksichtigt.

Die den Bewertungen zugrundegelegten Zeitangaben basieren auf mündlichen Angaben des Betreibers der Anlage. Es wurde auch hier eine konservative Abschätzung der für die Handlungen zur Verfügung stehenden Zeiten vorgenommen. Soweit zweckmäßig, werden die allgemeinen Annahmen, die der Bewertung zugrunde liegen, hier vorangestellt. Weitere Annahmen für die Verwendung einzelner Bewertungen werden bei den entsprechenden Handmaßnahmen genannt.

- Ergonomische Gestaltung der Warte

Es wird bei der Bewertung davon ausgegangen, daß für die ergonomische Gestaltung der Warte in etwa die gleichen Gestaltungsgrundsätze eingehalten wurden, wie sie in Kraftwerkswarten anzutreffen sind. Insbesondere wird davon ausgegangen, daß keine wesentlichen Verletzungen ergonomischer Anforderungen bezüglich der Arbeitsplatz-, -mittel- und -umgebungsgestaltung vorliegen (z.B. ungünstige Sichtverhältnisse bei wichtigen Anzeigen, hoher Lärm, Verletzung von Stereotypen etc.).

- Qualifikation und Aufgaben des Personals

Die vorliegende Bewertung geht davon aus, daß die Anlage von jeweils einer Person in der Warte und vor Ort gefahren wird. Dabei wird ein ergonomisch akzeptabler Schichtrhythmus vorausgesetzt. Der Bedienungsmann in der Warte führt das An- und Abfahren der Anlage im Beisein des Betriebsingenieurs, die Überwachung des Betriebes und das Einleiten von Gegenmaßnahmen bei Störungen durch.

Die Bedienungsperson vor Ort führt neben den Anlagenrundgängen mit Kontrolle der örtlichen Anzeigen und der Sichtkontrolle auf Schäden (z.B. Leckagen) vor allem diskontinuierliche Arbeiten wie das Einfüllen des Hexamins, das Entleeren der Nutsche sowie kleinere Reparaturarbeiten aus. Darüber hinaus soll sie bei Störungen, die von der Warte aus nicht behebbar sind, durch Eingriffe vor Ort (z.B. Schließen von Ventilen, Öffnen von Ablaßeinrichtungen) auf Weisung des Operateurs in der Warte Gegenmaßnahmen einleiten. Die Verständigung zwischen Operateur und Bediener vor Ort erfolgt über tragbare Sprechfunkgeräte. Es wird bei der Bewertung davon ausgegangen, daß bei dem vorhandenen Geräuschpegel der Anlage eine gute Verständlichkeit über das Sprechfunkgerät gegeben ist (Umgebungs-Geräuschpegel L nicht größer als höchstens 80 dB(A) $\geq$ L $\geq$ 75 dB(A)) und daß eine ständige Betriebsbereitschaft der Sprechfunkgeräte sichergestellt ist. Es wird

weiterhin vorausgesetzt, daß bei Beginn der Schicht eine Besprechung des Arbeitsablaufes zwischen Operateur und Anlagenrundgänger stattfindet. Nach den uns vorliegenden Informationen hält sich der Anlagenrundgänger in den Zeiten zwischen Rundgängen oder Arbeiten vor Ort in der Warte auf. Allerdings ist nicht bekannt, ob er Aufgaben in der Warte wahrnimmt und gegebenenfalls, welcher Art diese sind.

Es wird davon ausgegangen, daß der Operateur mindestens die Qualifikation eines Facharbeiters in der chemischen Industrie hat, der Bediener vor Ort dagegen keine spezifische fachliche Qualifikation besitzt, sondern für die Aufgaben angelernt wird. Operateur und Bediener erhalten nach unseren Informationen kein spezielles Training, insbesondere auch keine gezielte wiederkehrende Schulung für Störungssituationen. Die Durchführung solcher Schulungsmaßnahmen ist aus unserer Sicht jedoch nachdrücklich zu empfehlen, da dadurch eine deutliche Verbesserung der Verfügbarkeit und Sicherheit der Anlage erreicht werden kann. Ferner sollte darauf geachtet werden, daß die Warte höchstens kurzzeitig mit nur einer Person besetzt ist, in der Regel aber zwei Personen (Operateur und Anlagenrundgänger) anwesend sind. Bei Ausfall des Operateurs muß ein fachkundiger Ersatzmann kurzfristig abrufbar sein. Das gesamte Personal sollte über das Verhalten in Notsituationen regelmäßig belehrt werden.

- Organisatorische und administrative Maßnahmen

Nach den uns vorliegenden Informationen besteht die pauschale Vorschrift, daß die Anlage bei gravierenden Ausfällen im Betriebssystem abzufahren ist. Eine stärkere Differenzierung nach Art, Zeitpunkt und Reihenfolge zutreffender Maßnahmen wird empfohlen. Ferner sollte, soweit nicht ohnehin vorhanden, die Einführung eines Alarmierungskonzeptes für Störungen einschließlich klarer Kompetenzregelungen vorgesehen werden. Es wird davon ausgegangen, daß beim Schichtwechsel eine Informationsübergabe an die neue Schicht sichergestellt ist. Ferner

wird davon ausgegangen, daß organisatorische Maßnahmen für die Sicherstellung einer ständigen Rufbereitschaft fachkundigen Personals getroffen sind.

- Arbeitshilfsmittel

Soweit nicht ohnehin vorhanden, sollten schriftliche Arbeitshilfsmittel wie Betriebshandbuch, Schichtbuch sowie schriftliche Reparatur- und Freischaltanweisungen vorgesehen werden. Das Betriebshandbuch sollte Informationen über zulässige Betriebsbedingungen der Anlage, Bedeutung von Alarmen sowie Anweisungen über Art, Reihenfolge und Zeitpunkt der bei Störungen durchzuführenden Maßnahmen enthalten. Für die Überprüfung der richtigen Stellung von Handarmaturen vor dem Anfahren sollten geeignete Checklisten eingesetzt werden.

6.3.3.2 Daten und Einzelbewertungen

Bei der Bewertung wurde, wie eingangs erwähnt, auf die Angaben in /6-7/ zurückgegriffen. Um eine konservative Abschätzung vorzunehmen, wurden die dort aufgeführten Fehlhandlungswahrscheinlichkeiten in der Regel um einen Faktor 5 erhöht. In Fällen, in denen die Daten direkt übertragbar erschienen, wurden keine Modifikationen vorgenommen. In einigen speziellen Fällen mußte auf subjektive Schätzungen zurückgegriffen werden. Die Schätzung orientierte sich dabei an Bewertungen, die in /6-7/ für Situationen vorgenommen werden, in denen vergleichbare Einflußgrößen wie zeitlicher Streß oder drohende Gefahr vorliegen.

Eine Zusammenstellung der Daten zu den verschiedenen Fehlhandlungsarten gibt Tabelle 6.8 wieder. Die Unsicherheitsfaktoren wurden wie folgt abgeschätzt:

$$p_{50} < 10^{-2} \qquad K = 10$$

$$10^{-2} \leq p_{50} \leq 1 \qquad K = 5$$

Tab. 6.8:

Daten zur Bewertung menschlicher Fehlhandlungen (Median/Unsicherheitsfaktor K)

Art der Maßnahme	Bewertung
Fehljustieren eines Grenzwertes	$p_{50} = 1 \cdot 10^{-2}/5$
Nichtbeachten von Alarmen (Dieser Wert schließt direkt zugehörige einfache Handlungen ein, wenn keine besonderen Einflüsse zu berücksichtigen sind.)	$p_{50} = 5 \cdot 10^{-4}/10$
Nichtbetätigen einer Handarmatur vor Ort (ohne Zeitdruck und Gefährdung)	$p_{50} = 1 \cdot 10^{-2}/5$
Nichtbetätigen einer Handarmatur vor Ort (Zeitdruck und Gefährdung)	$p_{50} = 0{,}5/5$
Nichtentdecken einer nicht akustisch gemeldeten Meldelampe	$p_{50} = 0{,}25/5$
Unterlassen des Ablassens[1]):	
- kein Zeitdruck, allerdings vorher Versagen einer Reihe alternativer Gegenmaßnahmen	$p_{50} = 5 \cdot 10^{-3}/10$
- hoher Zeitdruck ($5' < T \leq 10'$)	$p_{50} = 5 \cdot 10^{-3}/10$
- sehr hoher Zeitdruck ($T \leq 5'$)	$p_{50} = 5 \cdot 10^{-2}/5$
Unterlassen der Abschaltung der Hexaminzufuhr (weitere Alternativen vorhanden, kein Zeitdruck)	$p_{50} = 1 \cdot 10^{-3}/10$
Unterlassen des Regelns von Hand bei Reglerausfall (weitere Alternativen vorhanden)	$p_{50} = 1 \cdot 10^{-3}/10$
Nichterkennen von Fehlern im Gasabzugssystem über Monitor	$p_{50} = 1 \cdot 10^{-2}/5$
Keine Entleerung der Nutsche vor Ort	$p_{50} = 1 \cdot 10^{-4}/10$
Nichtbeachten einer Analoganzeige, nachdem bereits ein Alarm angesprochen hat	$p_{50} = 5 \cdot 10^{-3}/10$

[1]) Die angegebene Bewertung gilt nur unter der Voraussetzung, daß die Operateure über die sicherheitstechnische Bedeutung der Alarme und die Notwendigkeit des sofortigen Ablassens informiert sind und diese Kenntnisse in regelmäßigen Abständen aufgefrischt werden. Falls die genannten Voraussetzungen nicht erfüllt sind, würden sich folgende Werte ergeben:

Unterlassen des Ablassens:

- sehr hoher Zeitdruck ($T \leq 5'$) $p_{50} = 0{,}3/5$
- hoher Zeitdruck ($5' < T \leq 10'$) $p_{50} = 3 \cdot 10^{-2}/10$

Diese Abschätzung versucht die Unsicherheiten zu berücksichtigen, die sich daraus ergeben, daß in der vorliegenden Untersuchung keine Detailanalyse der Arbeitsaufgaben vorgenommen werden konnte und die Übertragbarkeit der Daten nicht völlig gesichert ist.

- Fehljustieren von Grenzwerten

In der Anlage kommen sowohl analoge als auch binäre Meßwerterfassungsgeräte zum Einsatz. Die von diesen Geräten direkt oder indirekt abgeleiteten Grenzwerte dienen sowohl zur Anregung von automatischen Schaltmaßnahmen als auch zur Alarmierung. Eine Beschreibung der Einstellarbeiten an den Signalgeräten (Grenzwertmelder bzw. binäre Geber) lag nicht vor. Bei der Bewertung wird daher davon ausgegangen, daß die Arbeiten im wesentlichen analog zu entsprechenden Arbeiten in Kernkraftwerken durchgeführt werden, d.h., durch Simulation der Meßgröße bzw. des Meßsignals wird das korrekte Ansprechen des Grenzwertes kontrolliert. In deutschen Kernkraftwerken wird hierzu bei Analoggebern der gesamte Meßbereich des Meßumformers sowohl in steigender als auch in fallender Richtung durchfahren und das Ansprechen der Grenzwertgeber einschließlich ihrer Schalthysterese kontrolliert und protokolliert.

In /6-7/ wird für die unbemerkte Fehljustierung von Grenzwertmeldern (z.B. aufgrund eines defekten Meßgerätes) ein Wert von $p = 1 \cdot 10^{-2}/3$ angegeben. Dieser Wert wird für die Bewertung übernommen, lediglich der Irrtumsfaktor wegen der geringen Kenntnis der Arbeitsvorgänge auf 5 erhöht, so daß sich $p_{FJ} = 1 \cdot 10^{-2}/5$ ergibt. Eine Fehlerentdeckungsmöglichkeit (Faktor 10^{-1}) beim nachfolgenden Justieren eines weiteren Grenzwertes, wie in /6-7/ angegeben, wird hier pessimistisch nicht berücksichtigt, da der zeitliche und organisatorische Rahmen, in dem die Arbeiten ablaufen, nicht bekannt ist. Aus dem gleichen Grund wird eine eventuelle Abhängigkeit (Common Mode Failure) zwischen den Justierarbeiten an den verschiedenen Meßgeräten nicht berücksichtigt. Dies könnte möglicherweise zu

einer Unterschätzung des Einflusses von Fehljustierungen führen. Es wurde daher versucht, diesem Gesichtspunkt durch die bereits erwähnte Erhöhung des Irrtumsfaktors auf 5 Rechnung zu tragen.

In den Fehlerbäumen wurde der Ausfall der Meßeinrichtung aufgrund eines Hardwarefehlers mit dem Ausfall wegen Fehljustierens des Grenzwertes zusammengefaßt. Hierzu wurde die entsprechende Ausfallrate λ der Meßeinrichtung in eine Nichtverfügbarkeit $u \tilde{=} \lambda\theta/2$ (siehe Gleichung (5.4)) umgerechnet, wobei θ die Testzeit der Komponente angibt und mit der Ausfallwahrscheinlichkeit pro Anforderung aufgrund des Fehljustierens als logisches ODER zusammengefaßt wird. Damit ergibt sich eine Ersatz-Ausfallwahrscheinlichkeit pro Anforderung und der zugehörige Irrtumsfaktor entsprechend den Rechenregeln für die Summation von logarithmisch normalverteilten Größen (Abschnitt 6.4.3.1).

- Fehlerbaum 1

- OP FAL/01 KHM "Durchflußmeßalarm wird nicht beachtet"

  Der Alarm wird durch ein akustisches und optisches Signal gemeldet. Die optische Signalisierung erfolgt durch Blinklicht. Nach dem Quittieren weist ein Ruhiglicht auf das Anstehen des Alarmes hin. Bei der Bewertung wird ferner davon ausgegangen, daß die Meldung in Form eines eindeutigen Meldetextes zugeordnet zum Ort der Störung in der Warte erscheint.

  Für die Durchführung der Gegenmaßnahmen steht ca. 1 Stunde nach dem Alarm zur Verfügung. Aufgrund des Alarms soll die Reservepumpe gestartet, der Durchfluß kontrolliert und die Anlage unverzüglich abgefahren werden.

  In /6-7/ wird für das Nichtbeachten einer Meldung durch akustisches Signal ein Wert von $p = 10^{-4}$ angegeben. Für die Bewertung wird daher ein Wert $p = 5 \cdot 10^{-4}/10$ angesetzt.

- OP 40 GA-01B STN "Reservepumpe 40 GA-01B wird nicht von Hand gestartet"

  Auf die Notwendigkeit der Maßnahme wird durch einen Durchflußmeßalarm hingewiesen. Für die Maßnahme steht ca. 1 Stunde zur Verfügung. Die Maßnahme selbst ist sehr einfach. Die Bewertung in Anlehnung an /6-7/ liefert einen Wert von $p_{50} = 5 \cdot 10^{-4}/10$.

- OP CB2-1 40008SN "Handventil CB2-1 vor Betriebspumpe wird nicht geschlossen"

  Diese Maßnahme ist erforderlich, falls bei Ausfall der Betriebspumpe und beim Start der Reservepumpe die vor der Betriebspumpe angeordnete Rückschlagklappe nicht schließt. Es ist aus den bekannten Unterlagen nicht ersichtlich, wie der Ausfall der Rückschlagklappe erkannt werden könnte. Die Kontrolle der Durchflußmessung ist hierfür nicht ausreichend. Es wird deshalb abgeschätzt, daß das Handventil mit einer Wahrscheinlichkeit von $p_{50} = 1 \cdot 10^{-2}/5$ nicht schließt. Die Bewertung orientiert sich daran, daß hier einerseits relativ viel Zeit zur Störungssuche zur Verfügung steht (ca. 1 h), andererseits die Ursachenfindung bei der vorhandenen Instrumentierung sehr schwierig ist. Hinzu kommt, daß mit dem Stoppen der Hexaminzufuhr eine wesentlich einfachere Gegenmaßnahme gegeben ist. Eine relativ einfache Überwachung wäre durch eine Rückwärtslaufüberwachung oder eine Stellungsmeldung der Rückschlagklappen möglich.

- OP TAH 04 NB "Alarm wird nicht beachtet"

  Die Bewertung dieser Maßnahme in Anlehnung an /6-7/ ergibt $p_{50} = 5 \cdot 10^{-4}/10$.

- OP 40 DG 01 NB "Leckage bzw. Entleerung des Tanks wird bei Rundgang nicht bemerkt"

  Nach Informationen kann davon ausgegangen werden, daß in der Regel zweimal pro Schicht ein Anlagenrundgang des Bedieners vor Ort erfolgt. Die Leckage bzw. der abgesunkene

Füllstand muß im ungünstigsten Fall innerhalb einer Stunde entdeckt werden. Es ist nicht bekannt, ob Leckagen in einer Wanne aufgefangen oder in einen Gully abgeleitet werden, oder ob sie durch eine Lache am Boden erkennbar sind. Da die bedingte Wahrscheinlichkeit, daß die Leckage bzw. die Niveauabsenkung in der Zeit außerhalb der Anlagenrundgänge auftritt, bereits p = 1 - 2/8 = 0,75 beträgt und die Wahrscheinlichkeit eines Entdeckens beim Anlagenrundgang gering ist, wird das Nichtentdecken einer Leckage bzw. eines abgesunkenen Füllstandes pessimistisch mit p_{50} = 1/1 bewertet.

- Fehlerbaum 2

- PAL 06 40004 KHM A/B "Alarm des Druckschalters PSL 06 wird nicht beachtet"

  Die Bewertung erfolgt in gleicher Weise wie für OP FAL/01 KHM, also $p_{50} = 5 \cdot 10^{-4}/10$.

- 40 OP GA-02B STN "Pumpe 40-GA-02B wird nicht von Hand gestartet"

  Auf die Notwendigkeit der Durchführung dieser Maßnahme wird durch einen Druckalarm hingewiesen. Es stehen ca. 10-15 Minuten zur Verfügung. Alternativ, aber hier nachgeordnet, besteht die Möglichkeit, die Hexaminzufuhr zu stoppen. Der Ausfall des Handstarts der Pumpe wird mit einer Wahrscheinlichkeit von $p_{50} = 5 \cdot 10^{-4}/10$ bewertet.

- CB2-1 40003 SN "Handventil vor 40-GA-02A wird nicht geschlossen"

  Die Handmaßnahme entspricht weitgehend der Maßnahme OP CB2-1 40008 SN. Allerdings stehen hier nur ca. 10 Minuten zur Diagnose und Durchführung zur Verfügung. Zudem muß die Maßnahme vor Ort bei steigender Gefährdung vorgenommen werden. Es wird deshalb ein Wert p_{50} = 0,5/5 abgeschätzt.

- 41-KD 03 A/B KHM "Hexamin wird nicht von Hand gestoppt"

  Diese Maßnahme ist notwendig, wenn nach Ausfall der Betriebspumpe oder Entleerung des kalten Kühlmitteltanks die automatische Abschaltung und Hexaminzufuhr nicht erfolgt. Nach unserem Kenntnisstand kann der Erfolg der automatischen Abschaltung nur am Erlöschen einer Lampe im Bedienungsfeld der entsprechenden Förderschnecke erkannt werden. Da auf die Notwendigkeit des Abschaltens nicht hingewiesen wird, sondern die Durchführung der Maßnahme allein von der Sorgfalt und der Detailkenntnis des Operateurs abhängt, wird davon ausgegangen, daß nur ein relativ geringer Teil aller Operateure die Notwendigkeit der Handabschaltung erkennt. Dafür wird ein Wert von $p_{50} = 0,25/5$ abgeschätzt.

- Fehlerbaum 3

- OP AB 2-14139 OEN "Bypass-Ventil wird bei Alarm 'Temperatur hoch' nicht geöffnet"

  Bei Ansprechen des Alarms in der Warte stehen dem Personal nur ca. 10 Minuten zur Störungsdiagnose zur Verfügung. Währenddessen steigt die Gefährdung ständig. Die zugehörige Aktion "Öffnen des Bypass-Ventils" muß vor Ort in der Nähe der gefährdeten Komponente durchgeführt werden. Aufgrund der knappen zur Verfügung stehenden Zeit und der drohenden Gefahr wird ein Wert von $p_{50} = 0,5/5$ abgeschätzt.

- Fehlerbaum 4

- MB2-5 41002 SN "Handventil vor Betriebspumpe 41 GA-01A wird nicht geschlossen (vor Ort)"

  Diese Maßnahme wird erforderlich, falls bei Ausfall der Betriebspumpe und beim Start der Reservepumpe die vor der Betriebspumpe angeordnete Rückschlagklappe nicht schließt. Für diese Maßnahme steht ca. 1 Stunde zur Ver-

fügung. Die Bewertung erfolgt analog zu OP CB2-1 40008 SN mit $p_{50} = 1 \cdot 10^{-2}/5$.

- LAL 04 FAD 01A KHM "Niveau- und Durchflußalarm wird nicht beachtet"

  Beide Alarme weisen auf den HNO_3-Ausfall hin. Die zeitliche Aufeinanderfolge der Alarme konnte nicht eindeutig geklärt werden. Bei der Bewertung wird davon ausgegangen, daß die beiden Alarme in engem zeitlichen Abstand ansprechen. Für das Nichtbeachten der Alarme wird ein Wert von $p_{50} = 5 \cdot 10^{-4}/10$ abgeschätzt.

● Fehlerbaum 5

- OP 41 DC 01 AA LNA "Ablassen von Hand erfolgt nicht (vor Ort oder Warte), Fall A"

  Diese Maßnahme wird notwendig, wenn zuvor alle anderen Gegenmaßnahmen bei Ausfall des warmen Teils des Kühlmittelkreislaufes bzw. bei Ausfall der Salpetersäureversorgung erfolglos waren. Es wird bei der Bewertung davon ausgegangen, daß die Maßnahme zunächst von der Warte aus erfolgt. Die Maßnahme selbst ist sehr einfach (Knopfdruck). Da allerdings zuvor schon eine Reihe anderer Maßnahmen versagt haben, ist davon auszugehen, daß der Operateur unter sehr hohem Streß steht. Die Maßnahme ist ca. 1 Stunde nach Eintritt des auslösenden Ereignisses notwendig. Allerdings werden vorher eine Reihe anderer Maßnahmen versucht, um den Verlust einer ganzen Charge der Produktion zu vermeiden. Dies führt dazu, daß diese Maßnahme vermutlich sehr spät nach Versagen aller Alternativen durchgeführt wird. Da es sich um die zentrale sicherheitsgerichtete Maßnahme für alle Störungen handelt, kann von einer sehr hohen Vertrautheit der Operateure mit ihr ausgegangen werden. Es wird ein Wert von $p_{50} = 5 \cdot 10^{-3}/10$ abgeschätzt.

- HV01A 41026A OEN "Ablaßventil wird nicht von Hand geöffnet, Fall A"

  Diese Maßnahme wird notwendig, wenn die Abschaltung von der Warte aus oder vor Ort über Knopfdruck versagt hat. Dabei ist ein Handrad aufzudrehen, obwohl bereits sehr hohe Gefährdung besteht. Es wird hierfür ein Wert von $p_{50} = 0,5/5$ abgeschätzt.

- OP 41 DC01AA LNB "Ablassen von Hand erfolgt nicht (vor Ort oder Warte), Fall B"

  Diese Handmaßnahme unterscheidet sich von OP 41 DC01AA LNA dadurch, daß nur sehr geringe Zeit zur Verfügung steht. Sie wird erforderlich, wenn der Alarm des Rührers aufgrund einer zu geringen Drehzahl oder der Alarm des Nitrierers als Folge zu hoher Temperatur anspricht. Es wird davon ausgegangen, daß die Maßnahme, wie im Fall A, zunächst von der Warte aus versucht wird. Sie stellt die einzig mögliche sicherheitsgerichtete Gegenmaßnahme bei Rührerausfall und die Hauptmaßnahme bei Temperaturalarm dar (weitere Möglichkeit: Bypassventil öffnen). Es wird vorausgesetzt, daß der Operateur über die sicherheitstechnische Bedeutung des Alarms und die erforderliche Maßnahme informiert ist. Allerdings ist ein sehr hoher Streß aufgrund der drohenden Gefahr zu berücksichtigen. Es wird daher ein Wert von $p_{50} = 5 \cdot 10^{-2}/5$ für den Ausfall des Ablassens abgeschätzt.

- HV01A 41026B OEN "Ablaßventil wird nicht von Hand geöffnet, Fall B"

  Die Maßnahme unterscheidet sich von HV01A 41026A/B OEN nur durch die noch weitaus ungünstigeren zeitlichen Randbedingungen. Für den vorliegenden Fall wird diese Handmaßnahme als nicht zeitgerecht durchführbar angesehen. Daher wird ein Wert von $p_{50} = 1/1$ angesetzt.

- OP 41 KD03A/B KHM "Keine Handabschaltung der Hexaminzufuhr (vor Ort oder Warte)"

  Diese Maßnahme ist bei Ausfall der Nitrierkühlung (gemeinsamer warmer Teil) oder bei Ausfall der Salpetersäureversorgung erforderlich. Für die Maßnahme steht ausreichend Zeit zur Verfügung. Bei Nichterfolg sind weitere alternative Maßnahmen möglich. Es wird ein Wert von $p_{50} = 1 \cdot 10^{-3}/10$ abgeschätzt.

- OP TAH07 NB "Alarm wird nicht beachtet"

  Hierfür wird eine Wahrscheinlichkeit von $p_{50} = 5 \cdot 10^{-4}/10$ abgeschätzt.

- Fehlerbaum 6

- OP SAH04 NB "Alarm wird nicht beachtet"

  Hierfür wird eine Wahrscheinlichkeit von $p_{50} = 5 \cdot 10^{-4}/10$ abgeschätzt.

- OP SAL04 NB "Alarm wird nicht beachtet"

  Hierfür wird eine Wahrscheinlichkeit von $p_{50} = 5 \cdot 10^{-4}/10$ abgeschätzt.

- Fehlerbaum 7

Der Fehlerbaum enthält keine Handmaßnahme.

- Fehlerbaum 8

- OP TI05 NB "Anzeige/Alarm des Temperaturmeßinstruments wird nicht beachtet"

  Bei der Bewertung wird davon ausgegangen, daß zusätzlich zur vorhandenen Anzeige eine Alarmeinrichtung installiert wird. Bewertung wie OP SAH04 NB, also $p_{50} = 5 \cdot 10^{-4}/10$.

- OP TI540022 KHM "Ausfall von Gegenmaßnahmen von Hand bei Temperatur zu hoch"

  Als Gegenmaßnahme kommen hier nur Provisorien in Frage, für die eine halbe Stunde zur Verfügung steht. Da die Art der Gegenmaßnahmen nicht festgelegt ist und dafür unseres Wissens auch keine Vorkehrungen getroffen sind, wird eine geeignete Reaktion für äußerst unwahrscheinlich gehalten (p_{50} = 1/1). Aus der Praxis ist zwar eine erfolgreiche Maßnahme bekannt (Zugeben von Eis); derartige Aktionen dürften aber eher zufallsabhängig sein. Es wird deshalb ein Wert von p_{50} = 1/1 angesetzt.

- OP 40GA04B STN "Druckalarm nicht beachtet (keine Gegenmaßnahme, Start Pumpe B)"

  Bei Ansprechen des Druckalarmes, der auf den Ausfall der Kaltwasserförderpumpe A hinweist, ist das Reserveaggregat B in Betrieb zu nehmen. Hierfür stehen ca. 10 Minuten zur Verfügung. Da die Maßnahme selbst relativ einfach ist, kann davon ausgegangen werden, daß sie nach Erkennen des Druckalarms erfolgt. Es wird ein Wert von $p_{50} = 5 \cdot 10^{-4}/10$ abgeschätzt.

- OP CB2-1 40020 SN "Handventil vor 40 GA/04A wird nicht geschlossen (vor Ort)"

  Diese Maßnahme ist erforderlich, wenn nach Ausfall der Kaltwasserförderpumpe A und Start des zugehörigen Reserveaggregates B die vor der Pumpe A angeordnete Rückschlagklappe nicht schließt. Es stehen ca. 10 Minuten bei steigender Gefährdung für sie zur Verfügung. Da unseres Wissens die Fehlerursache nicht direkt festzustellen ist (keine Information über die Stellung der Rückschlagklappe), wird erwartet, daß die Maßnahme mit einer Wahrscheinlichkeit von p_{50} = 0,5/5 nicht durchgeführt wird.

- Fehlerbaum 9

- PAH12 41047 KHM "Druckalarm wird nicht beachtet und Motorventil wird nicht geöffnet"

  Hierfür wird eine Wahrscheinlichkeit von $p_{50} = 5 \cdot 10^{-4}/10$ abgeschätzt.

- Fehlerbaum 10

- HV03 41066A OEN "Ablaßventil wird nicht von Hand geöffnet (vor Ort), Fall A"

  Dies wäre als letzte Möglichkeit denkbar, sofern andere automatische Maßnahmen bereits versagt haben. Diese Maßnahme erfolgt unter höchstem Zeitdruck und bei sehr großer Gefährdung (extremer Streß). Es wird hierfür ein Wert von $p_{50} = 0,5/5$ abgeschätzt.

- HV03 41066B OEN "Ablaßventil wird nicht von Hand geöffnet (vor Ort), Fall B"

  Aufgrund der wesentlich ungünstigeren zeitlichen Randbedingungen wird die Maßnahme als nicht zeitgerecht durchführbar angesehen. Daher erfolgt eine Bewertung mit $p_{50} = 1/1$.

- Fehlerbaum 11

- OP TAH17 NB "Alarm wird nicht beachtet"

  Hierfür wird eine Wahrscheinlichkeit von $p_{50} = 5 \cdot 10^{-4}/10$ abgeschätzt.

- HV13 4173 RN "Handregelventil HV13 wird bei Temperaturalarm nicht betätigt (Warte)"

  Diese Maßnahme soll bei Anstehen des Temperaturalarms als erste erfolgen. Bei ausbleibendem Erfolg kann alternativ dazu der Kocherinhalt in den Notablaßtank entleert werden.

Für den Ausfall der Maßnahme wird eine Wahrscheinlichkeit von $p_{50} = 1 \cdot 10^{-3}/10$ abgeschätzt.

- OP41 DC03 ALN "Ausfall Handauslösung für Ablassen Kocher bei Temperatur-Alarm"

  Diese Maßnahme soll erfolgen, wenn bei Ansprechen des Temperaturalarms der Erfolg der Gegenmaßnahme HV13 4173 RN ausbleibt. Es stehen ca. 10 Minuten zur Verfügung. Die Maßnahme ist sehr einfach (Knopfdruck), erfolgt aber unter hohem Streß. Es wird davon ausgegangen, daß die Bedeutung der Maßnahme den Operateuren bekannt ist. Hierfür wird ein Wert von $p_{50} = 5 \cdot 10^{-3}/10$ abgeschätzt.

- OP 41047 KHM "Ausfall des Gasabzugsystems wird in der Warte nicht erkannt"

  Der Ausfall des Gasabzugsystems kann neben dem Druckmeßalarm auch anhand des Bildes der zur Überwachung des Gasabzuges eingesetzten Fernsehkamera festgestellt werden. Nähere Informationen zur Qualität, Eindeutigkeit und Verläßlichkeit dieser Bildinformation liegen uns nicht vor. Bei der Bewertung wird davon ausgegangen, daß das Fernsehbild regelmäßig und in kurzen Abständen kontrolliert wird und daß die Farbveränderung des überwachten Gases gut erkennbar ist. Es wird ein Wert von $p_{50} = 1 \cdot 10^{-2}/5$ abgeschätzt.

- OP 41047 ALN "Ausfall Einleiten des Entleerens (Warte oder vor Ort)"

  Diese Maßnahme wird erforderlich, wenn zuvor die Gegenmaßnahme "Öffnen des Motorventils 41113 MV" erfolglos blieb. Es stehen ca. 10 Minuten hierfür zur Verfügung. Die Maßnahme selbst ist den Operateuren gut vertraut. Es wird hierfür ein Wert von $p_{50} = 5 \cdot 10^{-3}/10$ abgeschätzt.

- OP SAH06 NB "Alarm wird nicht beachtet"

  Hierfür wird eine Wahrscheinlichkeit von $p_{50} = 5 \cdot 10^{-4}/10$ abgeschätzt.

- OP HV0341 066 "Ausfall Handauslösung für Ablassen Kocher bei Drehzahlalarm (Warte oder vor Ort)"

  Diese Maßnahme soll bei Ansprechen der Alarme "Rührerdrehzahl hoch" (Bruch der Rührerwelle) bzw. bei "Rührerdrehzahl tief" (Ausfall des Antriebes) von der Warte aus oder vor Ort erfolgen. Es stehen ca. 5 Minuten zur Verfügung. Es wird hierfür ein Wert von $p_{50} = 5 \cdot 10^{-2}/5$ abgeschätzt. Dabei wird vorausgesetzt, daß der Operateur über die sicherheitstechnische Bedeutung der Alarme und die Notwendigkeit des sofortigen Ablassens informiert ist.

- OP SAL06 NB "Alarm wird nicht beachtet und Umschaltung auf Pumpe B erfolgt nicht"

  Hierfür wird eine Wahrscheinlichkeit von $p_{50} = 5 \cdot 10^{-4}/10$ abgeschätzt.

- Fehlerbaum 12

- MB2-1 042019 SN "Handventil vor Pumpe A wird nicht geschlossen"

  Das Schließen des Handventils ist notwendig, wenn nach Ausfall der Förderpumpe A und nach dem Start der Pumpe B die vor der Pumpe A angeordnete Rückschlagklappe nicht schließt. Für die Maßnahme stehen ca. 10 Minuten zur Verfügung. Hierfür wird eine Wahrscheinlichkeit von $p_{50} = 0{,}5/5$ abgeschätzt.

- OP 42GA02B STN "Ausfall des Startens von Pumpe B trotz Alarm"

  Bei Ansprechen des Niveau-Alarms des Separiergefäßes 42 DF02 ist als erste Maßnahme der Start der Förderpumpe B vorgesehen. Es wird bei der Bewertung davon ausgegangen, daß das Nichtbeachten der Meldung den entscheidenden Beitrag zum Ausfall der gesamten Handmaßnahme liefert. Somit ergibt sich $p_{50} = 5 \cdot 10^{-4}/10$.

- OP 42GA03B STN "Ausfall der Umschaltung von Pumpe A auf Pumpe B bei Durchflußalarm"

  Bei Ausfall der Pumpe spricht in der Warte ein Durchflußalarm an. Der Operateur soll daraufhin Pumpe B starten. Es wird davon ausgegangen, daß das Nichtbeachten der Meldung den entscheidenden Beitrag zum Ausfall der gesamten Handmaßnahmen liefert. Somit ergibt sich $p_{50} = 5 \cdot 10^{-4}/10$.

- OP MB2104215 SN "Handventil vor Pumpe A wird nicht geschlossen"

  Die Maßnahme entspricht MB2-1 042019 SN. Es ergibt sich also $p_{50} = 0{,}5/5$.

- OP ME2642018 OEN "Bypass-Ventil ME2-6 wird bei Niveau-Alarm nicht geöffnet"

  Diese Maßnahme soll erfolgen, wenn nach Ansprechen des Niveaualarms und dem Start der Förderpumpe B das Niveau im Separiergefäß weiter steigt. Die Ursache kann dabei sowohl im Ausfall der Förderpumpe B als auch im Ausfall der Ablaufregelung liegen. Es stehen ca. 15 Minuten hierfür zur Verfügung, eine unmittelbare Gefährdung liegt also nicht vor. Es wird hierfür ein Wert von $p_{50} = 5 \cdot 10^{-3}/10$ (Nichtbeachten der Analoganzeige) unter der Voraussetzung angesetzt, daß eine entsprechende Analoganzeige in der Warte installiert wird.

- XV 01A 41117 KHM "Handumschaltung erfolgt nicht bei Ausfall der automatischen Umschaltung"

  Diese Maßnahme ist notwendig, falls die automatische Umschaltung ausfällt. Die Umschaltung erfolgt alle 6 Stunden. Hierzu muß jemand vor Ort anwesend sein, der die Nutsche entleert. Es kann davon ausgegangen werden, daß das Versagen der automatischen Umschaltung mit sehr hoher Wahrscheinlichkeit vom Personal vor Ort entdeckt wird. Hierfür wird ein Wert von $p_{50} = 10^{-4}/10$ abgeschätzt.

- OP 42DF02 NE "Auslauf des Separiergefäßes verstopft"

  Um ein Verstopfen des Auslaufes des Separiergefäßes zu verhindern, muß in etwa wöchentlichem Abstand der sich am Boden des Separiergefäßes ansammelnde Schlamm abgelassen werden. Bei der Bewertung wird davon ausgegangen, daß diese Maßnahme im Rahmen der vor dem Anfahren der Anlage durchzuführenden Instandhaltungsmaßnahmen entsprechend einem festen Instandhaltungsplan erfolgt. Es wird ferner vorausgesetzt, daß ihr Erfolg für das Bedienungspersonal erkennbar ist. Für diese Maßnahme wird ein Wert von $p = 1 \cdot 10^{-3}/10$ abgeschätzt.

6.4 Ergebnisse der quantitativen Fehlerbaumauswertung

6.4.1 Beurteilung der vorhandenen Systemauslegung

6.4.1.1 Explosion im Nitrierer

Die Tabelle 6.9 enthält quantitative Angaben zum unerwünschten Ereignis "Explosion im Nitrierer". Die Definition der dabei verwendeten Größen und ihre Zusammenhänge wurden bereits im Abschnitt 6.2.1 behandelt. Insgesamt ergibt sich eine erwartete Häufigkeit für eine Explosion im Nitrierer von

$$h = 4{,}0 \cdot 10^{-2}\ a^{-1}$$

Die Hauptbeiträge dazu ergeben sich aus folgenden störfallauslösenden Ereignissen;

- N1.1, Ausfall des Umformers mit 62,5 %
- N1.2, Ausfall der Temperaturmessung mit 4 %
- N2.1, Ausfall des Regelventils mit 3,3 %
- N2.2, Ausfall des Reglers mit 5 %
- N11.1, Ausfall des Rührermotors mit 2,4 %
- N11.2, Ausfall der Hydraulikversorgung mit 19 %

Alle anderen auslösenden Ereignisse liefern niedrigere Beiträge zur erwarteten Explosionshäufigkeit und beeinflussen deshalb kaum deren Gesamthäufigkeit.

Tab. 6.9:

Eintrittshäufigkeiten und bedingte Systemnichtverfügbarkeiten für die störfallauslösenden Ereignisse und Häufigkeiten des unerwünschten Ereignisses "Explosion im Nitrierer" (Erwartungswerte)

Störfallauslösende Ereignisse				Häufigkeit des auslösenden Ereignisses $s_j(a^{-1})$	System-Nichtverfügbarkeit u_j	Häufigkeit des unerwünschten Ereignisses $h_j(a^{-1})$
Ereignis Nr.	Ausgefallene Komponente für das auslösende Ereignis					
	Komponente	FB	Bezeichnung			
N1.1	TY7A41EB01ABVL	3	Umformer	$5,5 \cdot 10^{-1}$	$4,6 \cdot 10^{-2}$	$2,5 \cdot 10^{-2}$
N1.2	TE07A41EB01ABVL	3	Temperaturmessung	$3,1 \cdot 10^{-2}$	$4,6 \cdot 10^{-2}$	$1,4 \cdot 10^{-3}$
N2.1	TV07A41139BV	3	Regelventil	$2,5 \cdot 10^{-1}$	$5,0 \cdot 10^{-3}$	$1,3 \cdot 10^{-3}$
N2.2	TIC07A4139BVL	3	Regler	$3,9 \cdot 10^{-1}$	$5,0 \cdot 10^{-3}$	$2,0 \cdot 10^{-3}$
N3.1	TS.40001BV	1	Thermostatschalter	$3,2 \cdot 10^{-2}$	$1,2 \cdot 10^{-4}$	$3,8 \cdot 10^{-6}$
N3.2	40ED-01BV	1	Rückkühlsystem	1,8	$1,2 \cdot 10^{-4}$	$2,2 \cdot 10^{-4}$
N4	LE40010-40001	1	Leckage	$2,2 \cdot 10^{-2}$	$1,2 \cdot 10^{-4}$	$2,6 \cdot 10^{-6}$
N5	ROHRL.N.DRSCH	2	Leckage	$8,8 \cdot 10^{-4}$	$5,9 \cdot 10^{-3}$	$5,2 \cdot 10^{-6}$
N6	40GA-01ABV	1	warme Pumpe	$3,9 \cdot 10^{-1}$	$3,3 \cdot 10^{-4}$	$1,3 \cdot 10^{-4}$
N7	40GA-02ABV	2	kalte Pumpe	$3,9 \cdot 10^{-1}$	$6,3 \cdot 10^{-6}$	$2,5 \cdot 10^{-6}$
N8	41GA-01ABV	4	HNO_3-Pumpe	1,6	$3,1 \cdot 10^{-7}$	$5,0 \cdot 10^{-7}$
N9	41EB-01ALE	7	Leckage	$8,8 \cdot 10^{-4}$	1,0	$8,8 \cdot 10^{-4}$
N10	41GF-01ABR	6	Rührer	$1,8 \cdot 10^{-3}$	0,11	$2,0 \cdot 10^{-4}$
N11.1	41GF-01ABV	6	Rührermotor	$8,8 \cdot 10^{-3}$	0,11	$9,7 \cdot 10^{-4}$
N11.2	41GS-01BV	6	Hydraulikversorgung	$7,0 \cdot 10^{-2}$	0,11	$7,7 \cdot 10^{-3}$
Summe der Häufigkeit von Explosionen im Nitrierer:						$h = 4,0 \cdot 10^{-2}$

FB = Fehlerbaum

Ein auslösendes Ereignis trägt dann wenig zur Explosionshäufigkeit bei, wenn es selten eintritt, die Nichtverfügbarkeit der zu seiner Beherrschung erforderlichen Systeme (Systemfunktion) gering ist oder beide Bedingungen gleichzeitg erfüllt sind. Bei den vorliegenden Ergebnissen lassen sich folgende Fälle unterscheiden:

- Das störfallauslösende Ereignis ist relativ häufig, aber die für die Beherrschung erforderlichen Systeme sind gut ausgelegt (N8, N3.2 in Tabelle 6.9).
- Das störfallauslösende Ereignis hat eine geringe Eintrittshäufigkeit, die Nichtverfügbarkeit der erforderlichen Systeme ist relativ hoch (N9, N10 in Tabelle 6.9).

- Das störfallauslösende Ereignis hat eine geringe Eintrittshäufigkeit und die Nichtverfügbarkeit der zu seiner Beherrschung notwendigen Systeme liegt relativ niedrig (N5, N3.1 in Tabelle 6.9).

Betrachtet man die Nichtverfügbarkeit der zur Beherrschung erforderlichen Systeme, so fällt auf, daß sie im Falle der auslösenden Ereignisse N1.1, N1.2, N10, N11.1 und N11.2 besonders hoch liegt. Aus diesem Grunde werden die entsprechenden Minimalschnitte in Tabelle 6.10 aufgeführt.

Tab. 6.10:

Minimalschnitte von Systemfunktionen mit hoher Nichtverfügbarkeit beim Nitrierer

Störfallauslösende Ereignisse N1.1 oder N1.2		Störfallauslösende Ereignisse[1] N10, N11.1 oder N11.2	
Zusätzlich zum auslösenden Ereignis enthält der Minimalschnitt das Element	Zeitlich gemittelte Nichtverfügbarkeit	Zusätzlich zum auslösenden Ereignis enthält der Minimalschnitt das Element	Zeitlich gemittelte Nichtverfügbarkeit
TSH08A BV	$2{,}0\cdot10^{-2}$	OP41 DC01 AALNB	$8{,}1\cdot10^{-2}$
TSHH08A ABV	$2{,}0\cdot10^{-2}$	SAH 04A41 GF01 AKA	$2{,}0\cdot10^{-2}$
SV01A 41026 OEN	$2{,}7\cdot10^{-3}$	SV 01A 41026 OEN / HV 01A 41026 BOEN	$2{,}7\cdot10^{-3}$
TE08A BV	$1{,}2\cdot10^{-3}$	41 GFM 08A	$1{,}8\cdot10^{-3}$
HV01A 41026 OEN	$2{,}6\cdot10^{-4}$	OP SAH 04 NB	$1{,}3\cdot10^{-3}$
41 KD03 AIBSNA	$1{,}7\cdot10^{-4}$	HV 01A 41026 OEN	$2{,}6\cdot10^{-4}$
41 GFM 08A	$1{,}8\cdot10^{-3}$	41 KD03 AIBSNA	$1{,}7\cdot10^{-4}$
Gesamt	$4{,}6\cdot10^{-2}$	Gesamt	0,11

[1]) Die Angaben gelten für das auslösende Ereignis N10. Bei den Ereignissen N11.1 und N11.2 ist SAH 04A41 GF01 AKA durch SAL 04A41 GF01 AKA und OP SAH 04 NB durch OP SAL 04 NB mit denselben Nichtverfügbarkeiten zu ersetzen.

Es ist ersichtlich, daß bei beiden Systemfunktionen eine Reihe von Minimalschnitten auftreten, die außer dem auslösenden Ereignis nur ein weiteres Element enthalten. Besonders hohe Beiträge gehen im Falle der auslösenden Ereignisse N1.1 und N1.2 von den Temperaturschaltern des Notabschaltsystems TSH08A und

TSHH08A sowie im Falle der auslösenden Ereignisse N10, N11.1 und N11.2 von der Handmaßnahme OP41DC01 AALNB "Ablassen von Hand erfolgt nicht" (vgl. dazu Abschnitt 6.3.3.2) und dem Ausfall des Drehzahlalarms SAH 04 bzw. SAL 04 aus. Eine Diskussion darüber, wie diese Ergebnisse bei der Systemverbesserung berücksichtigt werden, erfolgt im Abschnitt 6.4.2.1.

6.4.1.2 Explosion im Kocher

Die Tabelle 6.11 enthält quantitative Angaben über das unerwünschte Ereignis "Explosion im Kocher". Die Analyse führt auf eine erwartete Häufigkeit für das Ereignis von

$$h = 4{,}2 \cdot 10^{-2}\ a^{-1}$$

Die Hauptbeiträge dazu stammen aus den folgenden auslösenden Ereignissen:

- K1.1, Ausfall des Motors des Kühlturmventilators mit 2,3 %
- K2.1, Ausfall des Meßumformers für die Kühlungsregelung mit 33,5 %
- K2.2, Ausfall der Temperaturmessung für die Kühlungsregelung mit 3,8 %
- K4.1, Ausfall des schwimmergesteuerten Einspeiseventils in der Bodentasse des Kühlturms mit 21,6 %
- K4.3, Fehlen des Speisewassers für das Ersetzen der Verdunstungsverluste im Kühlkreislauf mit 12,7 %
- K9.1, Ausfall des Hydraulikmotors für den Rührer mit 2,3 %
- K9.2, Ausfall der Hydraulikversorgung für den Rührer mit 18,5 %

Wie bereits im vorangehenden Abschnitt erläutert, lassen sich bei den Ereignissen, die wenig zur Häufigkeit der Explosion beitragen, die folgenden Fälle unterscheiden:

- Das störfallauslösende Ereignis hat eine relativ große Eintrittshäufigkeit. Die für seine Beherrschung notwendigen Systeme weisen eine geringe Nichtverfügbarkeit auf (aus-

Tab. 6.11:

Eintrittshäufigkeiten und bedingte Systemnichtverfügbarkeiten für die störfallauslösenden Ereignisse und Häufigkeiten des unerwünschten Ereignisses "Explosion im Kocher" (Erwartungswerte)

Störfallauslösende Ereignisse				Häufigkeit des auslösenden Ereignisses $s_j(a^{-1})$	System-Nichtverfügbarkeit u_j	Häufigkeit des unerwünschten Ereignisses $h_j(a^{-1})$
Ereignis Nr.	Ausgefallene Komponente für das auslösende Ereignis					
	Komponente	FB	Bezeichnung			
K1.1	40EG01MOTBV	8	Motor für Kühlturmventilator	$1{,}8\cdot10^{-1}$	$5{,}3\cdot10^{-3}$	$9{,}5\cdot10^{-4}$
K1.2	TSL0740EG01BVC	8	Temperaturschalter für Ventilatorsteuerung	$3{,}2\cdot10^{-2}$	$5{,}3\cdot10^{-3}$	$1{,}7\cdot10^{-4}$
K1.3	TSLL0840EG01BV	8	Temperaturschalter für Heizungssteuerung	$3{,}2\cdot10^{-2}$	$5{,}3\cdot10^{-3}$	$1{,}7\cdot10^{-4}$
K1.4	40EG01VENBR	8	Keilriemen für Kühlturmventilator	$1{,}5\cdot10^{-1}$	$5{,}3\cdot10^{-3}$	$8{,}0\cdot10^{-4}$
K2.1	TY1741DC03BVL	11	Meßumformer für Regelung Kocherkühlung	$5{,}5\cdot10^{-1}$	$2{,}6\cdot10^{-2}$	$1{,}4\cdot10^{-2}$
K2.2	TE1741DC03BV	11	Temperaturmessung für Kühlungsregelung	$6{,}1\cdot10^{-2}$	$2{,}6\cdot10^{-2}$	$1{,}6\cdot10^{-3}$
K3.1	TV1741169BVL	11	Regelventil für Kühlungsregelung	$2{,}5\cdot10^{-1}$	$5{,}7\cdot10^{-4}$	$1{,}4\cdot10^{-4}$
K3.2	TIC1741169BVL	11	Regler für Kühlungsregelung	$3{,}9\cdot10^{-1}$	$5{,}7\cdot10^{-4}$	$2{,}2\cdot10^{-4}$
K4.1	LCV0200760EN	8	Schwimmergesteuertes Einspeiseventil	1,7	$5{,}3\cdot10^{-3}$	$9{,}0\cdot10^{-3}$
K4.2	4001840022LE	8	Leckage im Kühlkreislauf	$2{,}5\cdot10^{-2}$	$5{,}3\cdot10^{-3}$	$1{,}3\cdot10^{-4}$
K4.3	40076BV	8	Einspeisewasser	1,0	$5{,}3\cdot10^{-3}$	$5{,}3\cdot10^{-3}$
K5	40GA04ABV	8	Betriebliche Kaltwasserförderpumpe	$3{,}9\cdot10^{-1}$	$1{,}2\cdot10^{-4}$	$4{,}7\cdot10^{-5}$
K6	41GDM2ABV	9	Ventilatormotor Gasabzug	$1{,}8\cdot10^{-1}$	$5{,}7\cdot10^{-7}$	$1{,}0\cdot10^{-7}$
K7.1	41GD02AKR	9	Keilriemen für Ventilator	$1{,}5\cdot10^{-1}$	$8{,}7\cdot10^{-4}$	$1{,}3\cdot10^{-4}$
K7.2	41113BL	9	Absorption	$1{,}8\cdot10^{-2}$	$8{,}7\cdot10^{-4}$	$1{,}6\cdot10^{-5}$
K8	41GF01BR	11	Rührerachse	$3{,}5\cdot10^{-3}$	$1{,}1\cdot10^{-1}$	$3{,}9\cdot10^{-4}$
K9.1	41GF03BV	11	Hydraulikmotor für Rührer	$8{,}8\cdot10^{-3}$	$1{,}1\cdot10^{-1}$	$9{,}7\cdot10^{-4}$
K9.2	41GS02BV	11	Hydraulikversorgung für Rührer	$7{,}0\cdot10^{-2}$	$1{,}1\cdot10^{-1}$	$7{,}7\cdot10^{-3}$
Summe der Häufigkeiten von Explosionen im Kocher:						$h = 4{,}2\cdot10^{-2}$

FB = Fehlerbaum

lösende Ereignisse K1.2, K1.3, K1.4, K3.1, K3.2, K5, K6, K7.1, K7.2 in Tabelle 6.11).

- Das störfallauslösende Ereignis hat eine relativ geringe erwartete Eintrittshäufigkeit, und die Systeme, die zu seiner Beherrschung benötigt werden, haben eine relativ hohe Nichtverfügbarkeit (K8 in Tabelle 6.11).
- Das störfallauslösende Ereignis hat eine relativ geringe erwartete Eintrittshäufigkeit und die Systeme, die zu seiner Beherrschung benötigt werden, haben eine geringe Nichtverfügbarkeit (K4.2 in Tabelle 6.11).

Aus Tabelle 6.11 ist zu ersehen, daß die Nichtverfügbarkeiten der zur Beherrschung der auslösenden Ereignisse notwendigen Systeme im Falle der auslösenden Ereignisse K2.1, K2.2, K8, K9.1 und K9.2 besonders hoch liegen. Aus diesem Grund werden in der Tabelle 6.12 die Minimalschnitte der zugehörigen Systemfunktionen aufgeführt.

Tab. 6.12:

Minimalschnitte von Systemfunktionen mit hoher Nichtverfügbarkeit beim Kocher

Störfallauslösende Ereignisse K2.1 oder K2.2		Störfallauslösende Ereignisse[1] K8, K9.1 oder K9.2	
Zusätzlich zum auslösenden Ereignis enthält der Minimalschnitt das Element	Zeitlich gemittelte Nichtverfügbarkeit	Zusätzlich zum auslösenden Ereignis enthält der Minimalschnitt das Element	Zeitlich gemittelte Nichtverfügbarkeit
TSH 18 41DC03 BV	$2{,}1 \cdot 10^{-2}$	OP SAH 06 NB	$1{,}3 \cdot 10^{-3}$
SV03 41066 OEN	$2{,}7 \cdot 10^{-3}$	SAH 06 41GF03 KA	$2{,}0 \cdot 10^{-2}$
41 GFM 08B	$1{,}8 \cdot 10^{-3}$	OP HVO 341066	$8{,}1 \cdot 10^{-2}$
HV03 41066 OEN	$5{,}2 \cdot 10^{-4}$	SV03 41066 OENB, HV03 41066 BOEN	$2{,}7 \cdot 10^{-3}$
		HV03 41066 OENB	$5{,}2 \cdot 10^{-4}$
		41 GFM 08B	$1{,}8 \cdot 10^{-3}$
Gesamt	$2{,}6 \cdot 10^{-2}$	Gesamt	0,11

[1]) Die Angaben gelten für das auslösende Ereignis K8. Bei den Ereignissen K9.1 und K9.2 ist SAH 06 41GF03 KA durch SAL 06 41GF03 KA und OP SAH 06 NB durch OP SAL 06 NB mit denselben Nichtverfügbarkeiten zu ersetzen.

Es ist offensichtlich, daß eine Reihe von Minimalschnitten auftreten, die außer dem auslösenden Ereignis nur ein weiteres Element enthalten. Besondere Beiträge zur Nichtverfügbarkeit der Systemfunktion gehen dabei im Falle der auslösenden Ereignisse K2.1 und K2.2 von einem Versagen des Temperaturschalters TSH 18 und bei den auslösenden Ereignissen K8, K9.1 und K9.2 von der Handmaßnahme OP HV0 341066 "Ausfall Handauslösung für Ablassen Kocher bei Drehzahlalarm (Warte oder vor Ort)" (vgl. dazu Abschnitt 6.3.3.2) und dem Ausfall des Drehzahlalarms SAH 06 bzw. SAL 06 aus. Die Berücksichtigung dieser Ergebnisse bei der Systemverbesserung wird im Abschnitt 6.4.2.2 behandelt.

6.4.1.3 Ausfall des hydraulischen Transportsystems

Die Tabelle 6.13 enthält die quantitativen Ergebnisse zum unerwünschten Ereignis "Ausfall des hydraulischen Transportsystems". Die erwartete Häufigkeit für seinen Eintritt beträgt

$$h = 1{,}4\ a^{-1}$$

Besonders große Beiträge zu diesem Wert gehen dabei von denjenigen auslösenden Ereignissen aus, die allein bereits zum Ausfall des Transportsystems führen und gleichzeitig eine relativ hohe Eintrittshäufigkeit haben. Im einzelnen erhält man:

- T1.1 Versagen des Reglers LC 4 für Ablaufregelung mit 11,3 %
- T3 Ausfall der Förderpumpe zur Vorlage mit 4,7 %
- T6 Versagen des Dreiwegeventils mit 62,3 %
- T7 Ausfall des Motorventils SV08 mit 9,9 %

Die genannten Ereignisse tragen zusammen 88 % zur Ausfallhäufigkeit des Systems bei. Weitere größere Beiträge stammen aus den Ereignissen

Tab. 6.13:

Eintrittshäufigkeiten und bedingte Systemnichtverfügbarkeiten für die störfallauslösenden Ereignisse und Häufigkeiten des unerwünschten Ereignisses "Ausfall des hydraulischen Transportsystems" (Erwartungswerte)

Störfallauslösende Ereignisse				Häufigkeit des auslösenden Ereignisses $s_j(a^{-1})$	System-Nichtverfügbarkeit u_j	Häufigkeit des unerwünschten Ereignisses $h_j(a^{-1})$
Ereignis Nr.	Ausgefallene Komponente für das auslösende Ereignis					
	Komponente	FB	Bezeichnung			
T1.1	LC42DF02BVL	12	Regler für Ablaufregelung	1,7	$9,5 \cdot 10^{-2}$	$1,6 \cdot 10^{-1}$
T1.2	LV0342016BVL	12	Regelventil LV03 fällt aus	$5,0 \cdot 10^{-1}$	$9,5 \cdot 10^{-2}$	$4,8 \cdot 10^{-2}$
T1.3	LV0342016DLA	12	Druckluftversorgung für Regelventil	$5,7 \cdot 10^{-1}$	$9,5 \cdot 10^{-2}$	$5,4 \cdot 10^{-2}$
T2	XV01A41117AU	12	Automatische Umschaltung	$2,6 \cdot 10^{-2}$	$2,7 \cdot 10^{-4}$	$7,0 \cdot 10^{-6}$
T3	42GA02ABV	12	Förderpumpe zur Vorlage	$7,7 \cdot 10^{-1}$	$8,6 \cdot 10^{-2}$	$6,6 \cdot 10^{-2}$
T4	42GA03ABV	12	Förderpumpe (Förderkreislauf)	$3,9 \cdot 10^{-1}$	$2,8 \cdot 10^{-2}$	$1,1 \cdot 10^{-2}$
T5	42021BR	12	Bruch der Förderleitung	$8,8 \cdot 10^{-4}$	1,0	$8,8 \cdot 10^{-4}$
T6	XV01A41117SNU	12	Dreiwegeventil	$8,8 \cdot 10^{-1}$	1,0	$8,8 \cdot 10^{-1}$
T7	SV0841102BV	12	Motorventil SV08	$1,4 \cdot 10^{-1}$	1,0	$1,4 \cdot 10^{-1}$
T8	LSLH04BV	12	Niveaumesser im Aufgabetrichter	$5,0 \cdot 10^{-2}$	1,0	$5,0 \cdot 10^{-2}$
T9	OP42DF02NE	12	Auslauf des Separiergeräts verstopft	$2,7 \cdot 10^{-3}$	1,0	$2,7 \cdot 10^{-3}$
Summe der Häufigkeiten von Ausfällen des hydraulischen Transportsystems:						h = 1,4

FB = Fehlerbaum

- T1.2 Ausfall des Regelventils LV03 mit 3,4 %
- T1.3 Ausfall der Druckluftversorgung für das Regelventil mit 3,8 %
- T8 Nivaumesser im Aufgabetrichter fällt aus mit 3,6 %

Die Verbesserungsvorschläge, die sich aus den genannten Beiträgen ergeben, werden im Abschnitt 6.4.2.3 dargestellt.

6.4.2 Vorschläge zur Systemverbesserung und ihre Auswirkungen auf die Eintrittshäufigkeiten der unerwünschten Ereignisse

6.4.2.1 Nitrierer

Wie aus der Ergebnisanalyse im Abschnitt 6.4.1.1 ersichtlich, stammen die hauptsächlichen Beiträge zur Explosionshäufigkeit aus den Bereichen Kühlungsregelung (auslösende Ereignisse: N1.1, N1.2, N2.1, N2.2) mit insgesamt 74,8 % und Rührer (auslösende Ereignisse: N11.1 und N11.2) mit 21,4 %.

Kühlkreislauf und Rückkühlung sind hingegen gut ausgelegt, wie an den entsprechend niedrigen Werten für die Nichtverfügbarkeit der Systeme, die bei störfallauslösenden Ereignissen in diesen Bereichen benötigt werden, abzulesen ist.

Gleiches gilt im Zusammenhang mit auslösenden Ereignissen, welche die Salpetersäurezufuhr betreffen. Dies ist wahrscheinlich darauf zurückzuführen, daß ein sicherer Prozeßablauf und eine gute Produktausbeute nur bei Salpetersäureüberschuß erreicht werden können, so daß dessen Sicherstellung besondere Aufmerksamkeit beim Anlagenentwurf gewidmet wurde.

Um ein ausgewogenes Sicherheitskonzept zu verwirklichen, d.h. möglichst gleich hohe Beiträge aus jedem der Abläufe zum unerwünschten Ereignis zu erreichen, muß im vorliegenden Fall die Nichtverfügbarkeit der Systeme, die zur Beherrschung der eingangs genannten auslösenden Ereignisse vorgesehen sind, herabgesetzt werden. Bezüglich der störfallauslösenden Ereignisse N1.1 und N1.2 könnte dies nach den in der Tabelle 6.10 aufgeführten Ergebnissen vor allem durch eine Verbesserung bei den Grenzwertgebern TSH 08A und TSHH 08A erreicht werden. Diese ist jedoch gerätetechnisch nur schwer zu verwirklichen. Darüber hinaus ist zu bedenken, daß der wesentliche Teil der Nichtverfügbarkeit (80 %) auf die Möglichkeit eines Kalibrierfehlers zurückzuführen ist. Dadurch würde auch der Verfügbarkeitsgewinn durch Einbau redundanter Instrumente stark ge-

schmälert, da ein Common-Mode-Fehler beim Kalibrieren berücksichtigt werden müßte.

Aus diesem Grund wird vorgeschlagen, den Bypass über einen Temperaturschalter und ein Magnetventil beim Überschreiten der maximal zulässigen Temperatur vollständig zu öffnen. Dadurch wäre ein redundantes System zum normalen betrieblichen Regelsystem der Kühlung geschaffen, das überdies den Vorteil hätte, daß es bei Störungen der Kühlungsregelung nicht in jedem Falle sofort zum Notablassen und damit zum Produktverlust käme. Die vorgeschlagene Änderung läßt sich mit geringem Aufwand verwirklichen. Ihre Auswirkungen auf die Fehlerbäume sind in Bild 6.16 dargestellt.

Zur Quantifizierung der neuen Konfiguration wurden die folgenden Ausfallraten bzw. -wahrscheinlichkeiten verwendet:

- Temperaturschalter TSH

  $\lambda_{50} = 3{,}9 \cdot 10^{-6}\ h^{-1}/K = 6,$

  Wartungsintervall $\theta = 672$ h

- Magnetventil SV

  $\lambda_{50} = 21 \cdot 10^{-6}\ h^{-1}/K = 4{,}5,$

  Wartungsintervall $\theta = 168$ h

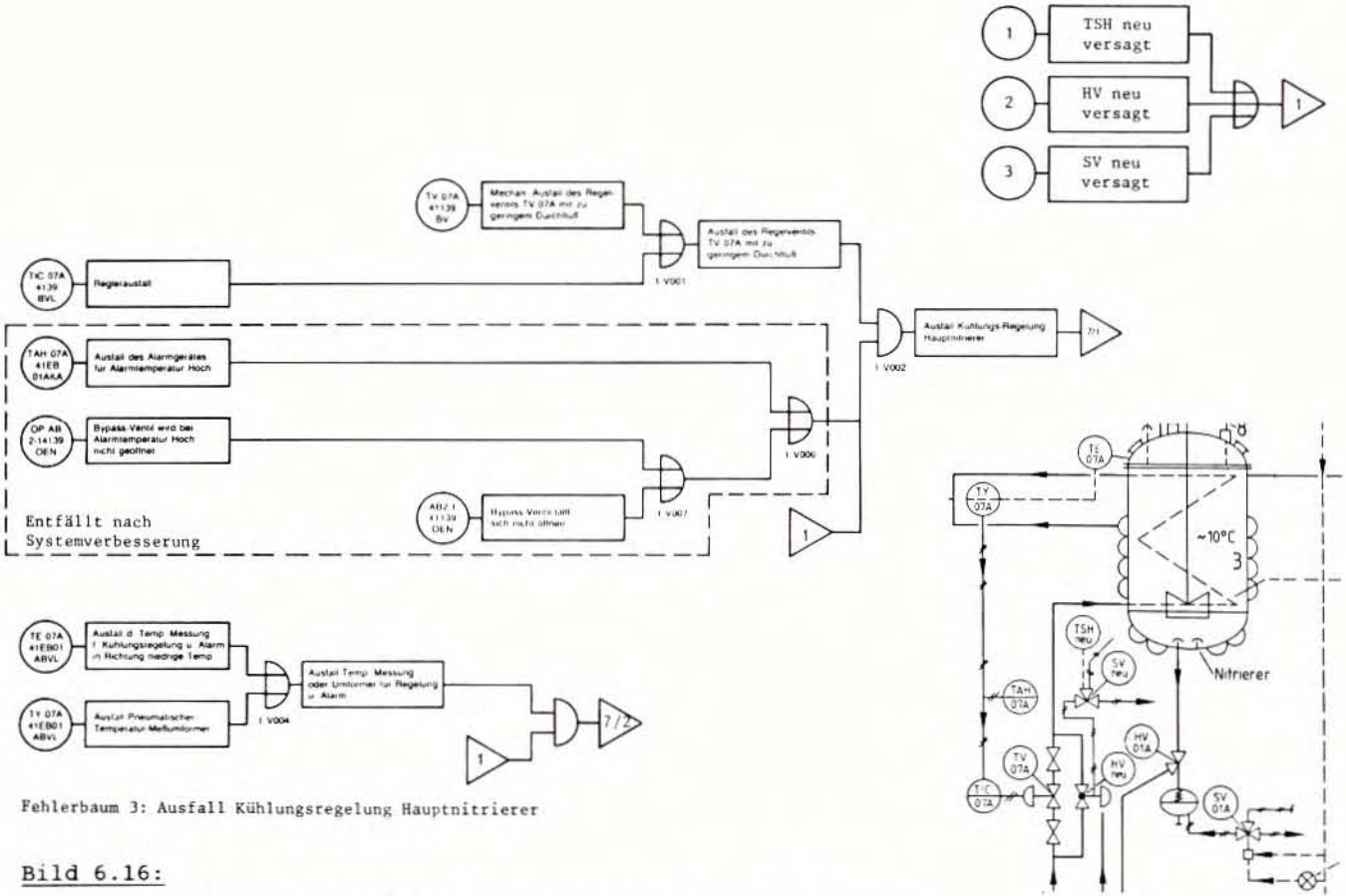
- Regelventil RV

  $\lambda_{50} = 29 \cdot 10^{-6}\ h^{-1}/K = 5,$

  Wartungsintervall $\theta = 168$ h

Die Ausfallrate für den Temperaturschalter ist dabei durch Multiplikation des für Wasser zutreffenden Wertes mit einem Medienbelastungsfaktor 2 entstanden. Zusätzlich zum Ausfall des Instrumentes wird ein Kalibrierfehler mit einer Wahrscheinlichkeit von $p_{50} = 0{,}01/5$ berücksichtigt.

Aufgrund der Systemänderung ergeben sich die folgenden Verfügbarkeitsgewinne:



Fehlerbaum 3: Ausfall Kühlungsregelung Hauptnitrierer

Bild 6.16:

Fehlerbaumänderungen als Folge der Automatisierung des Bypasses am Nitrierer

- Reduzierung der Nichtverfügbarkeit der Systeme, die zur Beherrschung der auslösenden Ereignisse N1.1 und N1.2 benötigt werden, von $4,6 \cdot 10^{-2}$ auf $1,2 \cdot 10^{-3}$;
- Reduzierung der Nichtverfügbarkeit der Systeme, die zur Beherrschung der auslösenden Ereignisse N2.1 und N2.2 benötigt werden, von $5 \cdot 10^{-3}$ auf $1,6 \cdot 10^{-4}$.

Den wesentlichen Beitrag zur Nichtverfügbarkeit der zur Beherrschung der störfallauslösenden Ereignisse N10, N11.1 und N11.2 liefert das Handablassen des Nitrierers OP41DC01AALNB. Es liegt daher nahe, das Ablassen direkt durch die Drehzahlalarmgeräte SAH 04 und SAL 04 auszulösen. Die entsprechende Änderung des Fehlerbaums wird in Bild 6.17 gezeigt. Dadurch reduziert sich die Nichtverfügbarkeit der Systemfunktion von 0,11 auf $2,5 \cdot 10^{-2}$. Auch diese Veränderung des Systems läßt sich ohne großen Aufwand verwirklichen.

Die Gesamtheit der vorgeschlagenen Verbesserungen führt dazu, daß sich die erwartete Eintrittshäufigkeit des unerwünschten Ereignisses von

$$h = 4,0 \cdot 10^{-2}\ a^{-1} \text{ auf } h' = 4,1 \cdot 10^{-3}\ a^{-1}$$

reduziert, wobei nunmehr die größten Beiträge (51 %) von Störungen vom Bereich des Rührers ausgehen.

6.4.2.2 Kocher

Die Ergebnisdarstellung im Abschnitt 6.4.1.2 weist aus, daß die wesentlichen Beiträge zur erwarteten Häufigkeit einer Explosion im Kocher aus den Bereichen Rückkühlung des Kühlwassers (Kühlturm) (39,6 %), Kühlungsregelung (38,2 %) und Rührer (21,7 %) stammen. Der hohe Beitrag der Rückkühlung ergibt sich insbesondere aus Mängeln beim Ersetzen verdunsteten Kühlwassers, da die entsprechenden Eintrittshäufigkeiten für die auslösenden Ereignisse relativ groß sind (K4.1, K4.3). Obwohl die Nichtverfügbarkeit der notwendigen Systeme zur Beherrschung

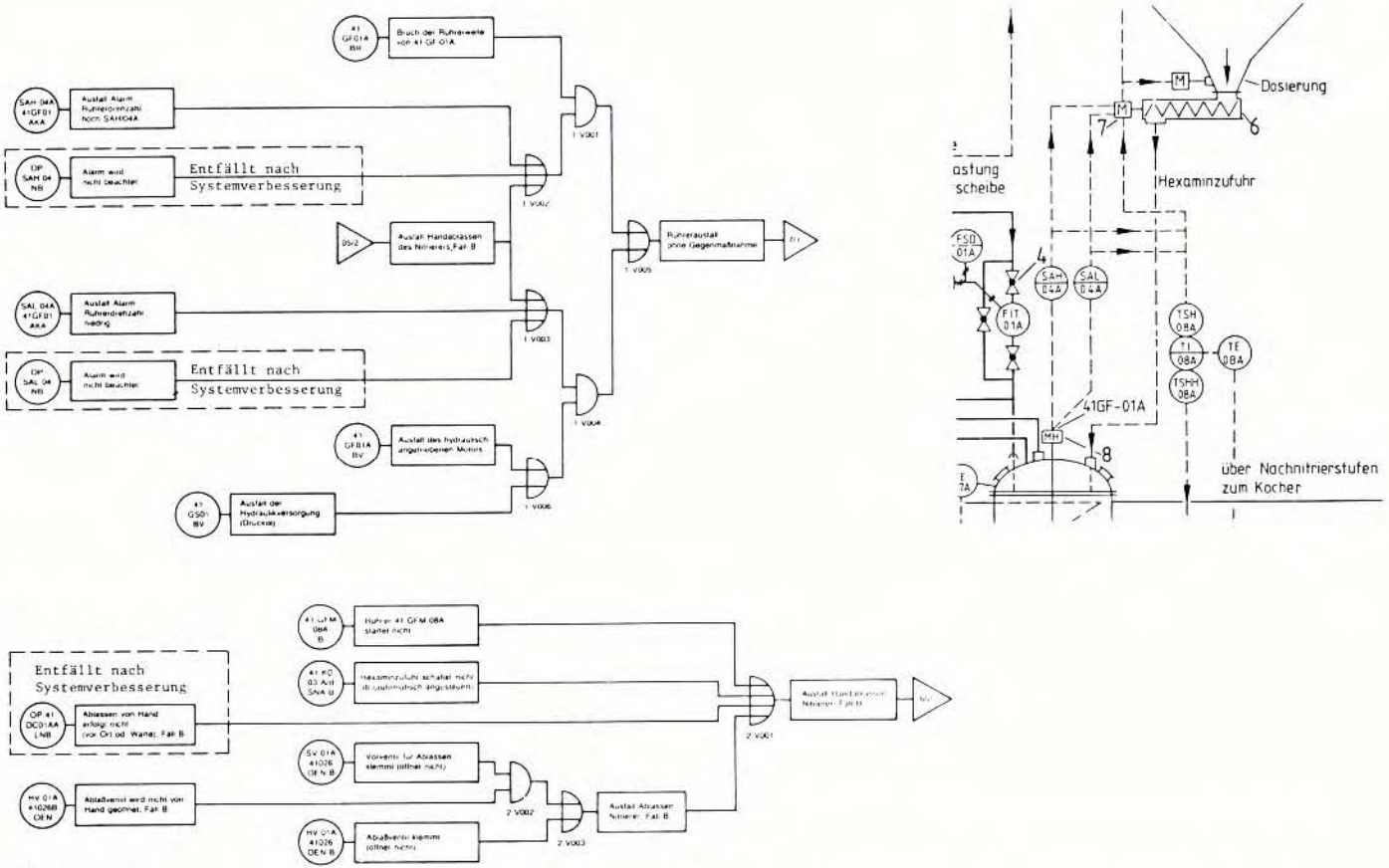


Bild 6.17:

Fehlerbaumänderungen als Folge der Automatisierung des Einleitens des Notablassens bei zu hoher und zu niedriger Drehzahl des Rührers des Nitrierers

der genannten auslösenden Ereignisse nicht besonders hoch liegt, kann hier Abhilfe nur durch eine weitere Reduzierung geschaffen werden. Dies läßt sich erreichen, indem man einen Alarm bei niedrigem Niveau in der Kühlturmtasse vorsieht, der mit einer geeigneten Handmaßnahme gekoppelt wird (Ventilreparatur, Wasserbeschaffung aus anderen Quellen, Abfahren der Anlage etc.). Wie sich die Änderung auf den Fehlerbaum auswirkt, wird in Bild 6.18 gezeigt.

Wird für das Alarmgerät eine Ausfallrate $\lambda_{50} = 4 \cdot 10^{-6}\ h^{-1}/K = 4$ und ein zugehöriges Wartungsintervall von $\theta = 672$ h benutzt und für das Versagen der Handmaßnahme eine Wahrscheinlichkeit von $p_{50} = 5 \cdot 10^{-4}/K = 10$ angesetzt, so reduziert sich die Nichtverfügbarkeit der Systemfunktion für die auslösenden Ereignisse K4.1, K4.2 und K4.3 von

$$5{,}3 \cdot 10^{-3} \text{ auf } 1{,}7 \cdot 10^{-5}$$

Bezüglich der störfallauslösenden Ereignisse K2.1 und K2.2 gelten die Ausführungen des vorangehenden Abschnitts entsprechend. Auch hier wird eine Automatisierung des Bypasses des Kühlsystems vorgeschlagen. Die daraus sich ergebenden Fehlerbaumänderungen werden in Bild 6.19 dargestellt.

Für die Komponenten werden dieselben Ausfallraten, -wahrscheinlichkeiten und Wartungszeiten wie im vorangehenden Abschnitt benutzt. Nur beim Temperaturschalter wird wegen der höheren Temperatur und dadurch verstärkten Korrosion der dortige Wert mit einem Medieneinflußfaktor 2 multipliziert, so daß sich

$$\lambda_{50} = 7{,}7 \cdot 10^{-6}\ h^{-1}/K = 6$$

ergibt. Die vorgeschlagene Systemänderung hat folgenden Einfluß:

- Reduzierung der Nichtverfügbarkeit der Systeme, die zur Beherrschung der auslösenden Ereignisse K2.1 und K2.2 benötigt werden, von $2{,}6 \cdot 10^{-2}$ auf $7{,}1 \cdot 10^{-4}$;

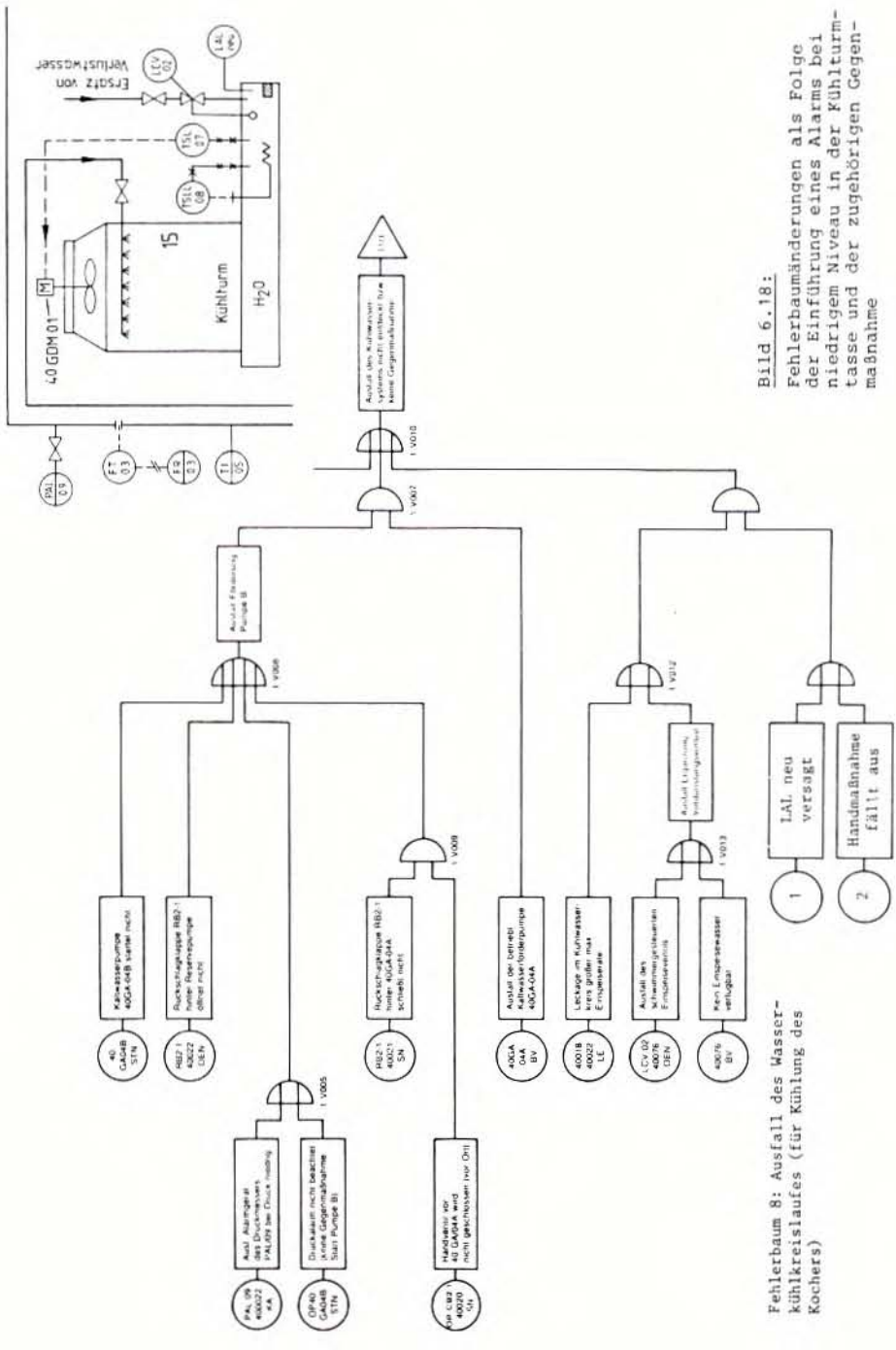


Bild 6.18:
Fehlerbaumänderungen als Folge der Einführung eines Alarms bei niedrigem Niveau in der Kühlturmtasse und der zugehörigen Gegenmaßnahme

Fehlerbaum 8: Ausfall des Wasserkühlkreislaufes (für Kühlung des Kochers)

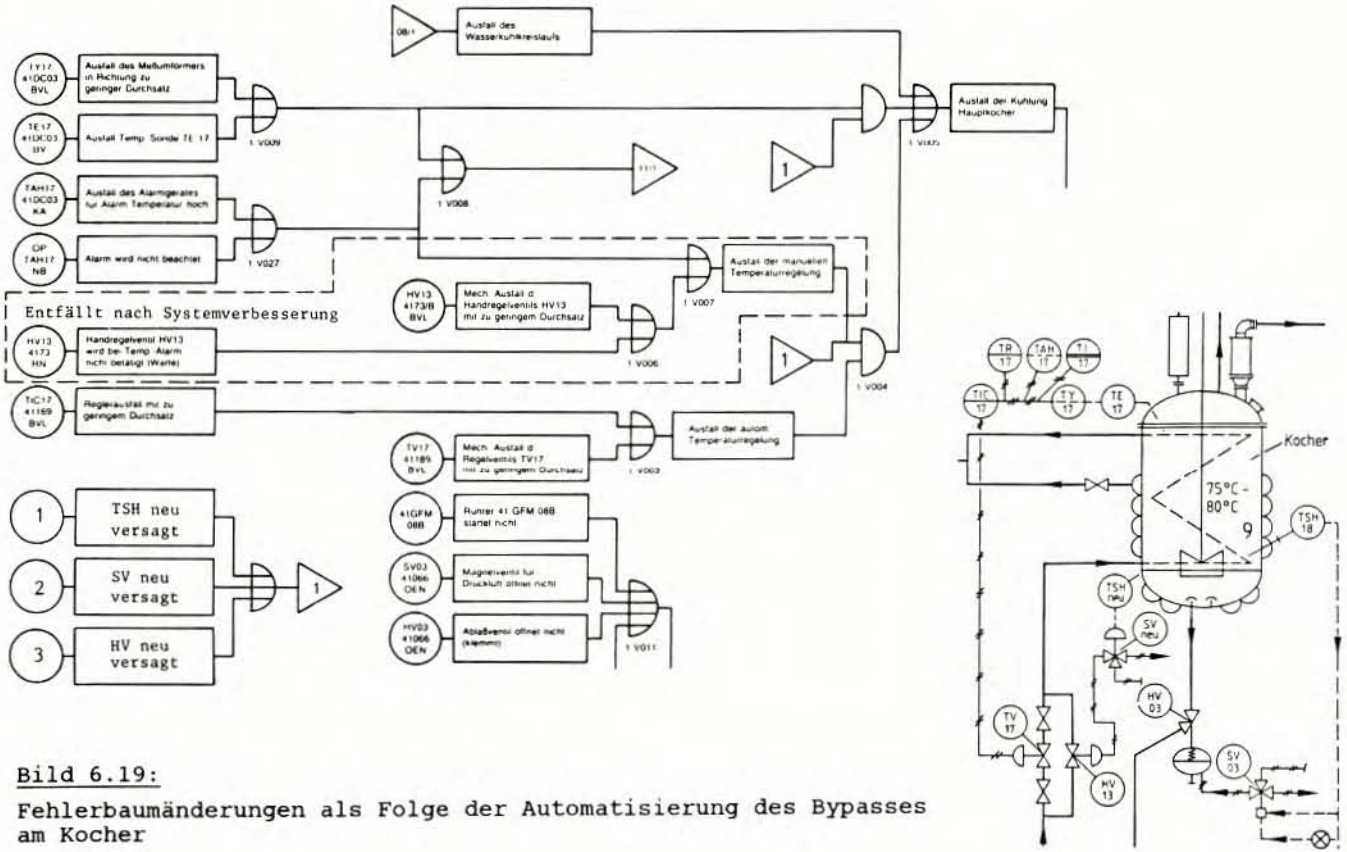


Bild 6.19:

Fehlerbaumänderungen als Folge der Automatisierung des Bypasses am Kocher

- Reduzierung der Nichtverfügbarkeit der Systeme, die zur Beherrschung der auslösenden Ereignisse K3.1 und K3.2 benötigt werden, von $5,7 \cdot 10^{-4}$ auf $1,7 \cdot 10^{-5}$.

Auch in bezug auf diejenigen störfallauslösenden Ereignisse, die den Rührer betreffen (K8, K9.1 und K9.2), kann auf die Ausführungen des vorangehenden Abschnitts zurückgegriffen werden. Die Auswirkungen der dabei vorgesehenen Automatisierung des Einleitens des Notablassens auf die Fehlerbäume werden in Bild 6.20 gezeigt. Durch sie wird die Nichtverfügbarkeit der zur Beherrschung notwendigen Systeme von

$$0,11 \text{ auf } 2,6 \cdot 10^{-2}$$

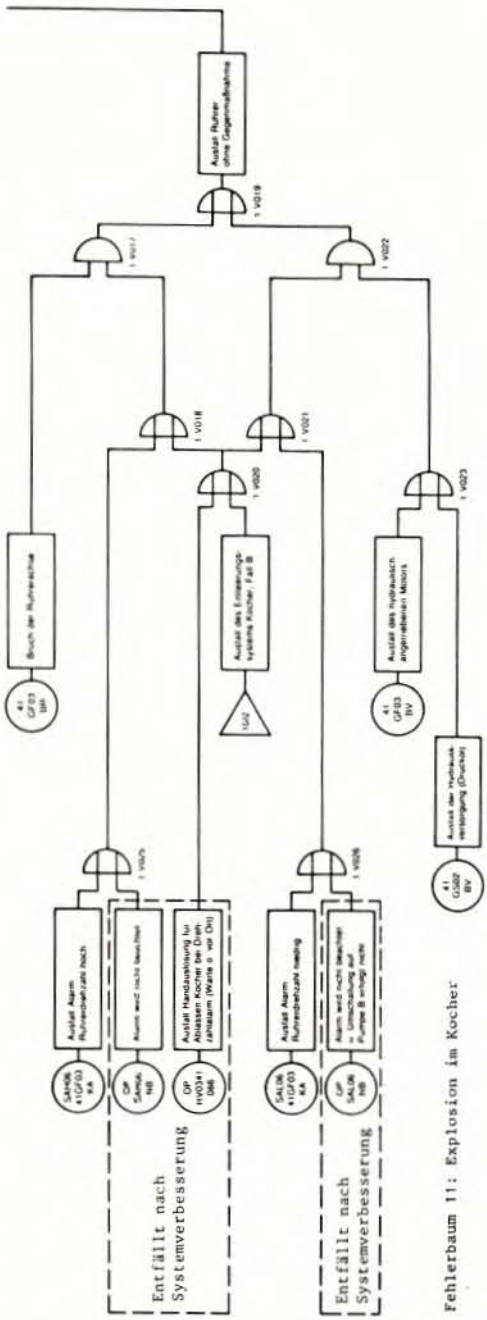
herabgesetzt.

Die vorgeschlagenen Systemverbesserungen lassen sich mit geringem Aufwand verwirklichen. Sie führen insgesamt zu einer Herabsetzung der erwarteten Häufigkeit einer Explosion im Kocher von

$$h = 4,2 \cdot 10^{-2}\ a^{-1} \text{ auf } h' = 4,9 \cdot 10^{-3}\ a^{-1}$$

6.4.2.3 Hydraulisches Transportsystem

Gemäß der Aufschlüsselung des Abschnitts 6.4.1.3 stammen die wesentlichen Beiträge zur Ausfallhäufigkeit des Systems aus dem Versagen von Komponenten, die allein bereits den Systemausfall hervorrufen können. Einen besonders großen Anteil hat daran das Versagen des Dreiwegeventils XV01. Es läge daher nahe, dieses Ventil durch zwei normale Absperrventile zu ersetzen, von denen eines den Weg zur Nutsche freigibt, während das andere den Weg zum zweiten Stabilisator sperrt und umgekehrt bei Wechsel des Betriebszustandes. Angesichts der Tatsache, daß die Ausfallrate für das Dreiwegeventil geschätzt werden mußte, läßt sich nicht mit Sicherheit feststellen, ob eine solche Änderung tatsächlich zu einer Verminderung der Ausfallhäufigkeit führen würde.



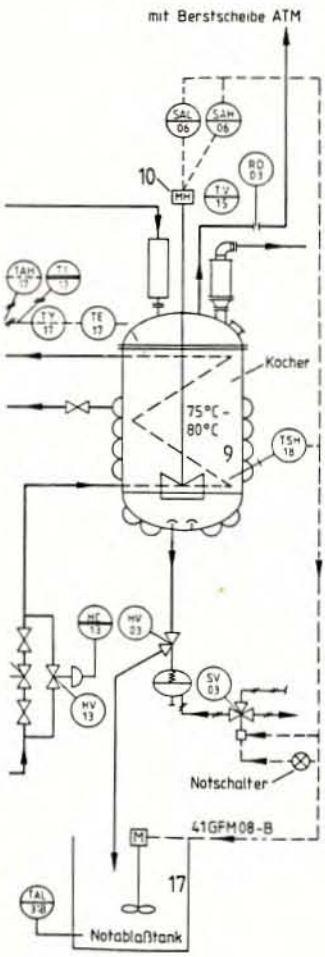


Bild 6.20:

Fehlerbaumänderungen als Folge der Automatisierung des Einleitens des Notablassens bei zu hoher und zu niedriger Drehzahl des Rührers des Kochers

Da auch zahlreiche weitere Ausfallraten bei diesem System geschätzt werden mußten, ist seine zuverlässige probabilistische Beurteilung erst möglich, wenn entsprechende ausgewertete Betriebserfahrung vorliegt. Dann könnten auch tragfähige Vorschläge zur Reduzierung seiner Ausfallhäufigkeit gemacht werden. Die aufgeführten Ergebnisse sind somit lediglich als grobe Abschätzung aufzufassen.

6.4.3 Unsicherheiten

6.4.3.1 Allgemeines

Die Ergebnisse der vorangehenden Analyse sind mit Unsicherheiten behaftet. Diese betreffen zum einen die Modellierung der untersuchten Systeme durch Fehlerbäume und zum anderen die zu deren Quantifizierung verwendeten Ausfallraten bzw. -wahrscheinlichkeiten für technische Komponenten und menschliches Fehlverhalten.

Während es schwierig oder gar unmöglich ist, die Unsicherheiten aus der Modellierung zu quantifizieren, da weder durch das vorliegende noch durch irgendein anderes Verfahren sichergestellt werden kann, daß wirklich alle relevanten Ereignisabläufe im Modell berücksichtigt worden sind, läßt sich die Auswirkung der Unsicherheiten bei den Eingangsdaten auf das Endergebnis ermitteln. Dadurch erhält man ein Maß für dessen Güte.

Die Unsicherheiten der Daten werden in der vorliegenden Arbeit durch logarithmische Normalverteilungen beschrieben (Abschnitt 5.2). Bei der Auswertung von Fehlerbäumen treten Summen und Produkte dieses Verteilungstyps auf. Sie werden mit Hilfe der folgenden Beziehungen gebildet /6-11/:

- Summe logarithmisch normalverteilter Variablen

Die Summe logarithmisch normalverteilter Variablen führt nicht auf eine logarithmische Normalverteilung. Sie läßt sich jedoch

im allgemeinen durch eine logarithmische Normalverteilung annähern. Die Berechnung der entsprechenden Verteilungsparameter wird nachfolgend am Beispiel zweier unabhängiger Zufallsgrößen X und Y erläutert.

Sind x_{50} der Median und K_x der Unsicherheitsfaktor einer logarithmischen Normalverteilung für X, so lautet deren Erwartungswert

$$E(X) = x_{50} \cdot \exp(\varepsilon_x^2/2) \tag{6.1}$$

wobei

$$\varepsilon_x = \ln K_x/1{,}645 \text{ [1)}$$

Für die zugehörige Streuung gilt:

$$D^2(Y) = (E(X))^2 \, [\exp(\varepsilon_x^2)-1] \tag{6.2}$$

Entsprechende Beziehungen gelten für die Variable Y.

Als Parameter der Verteilung der Summe Z = X + Y gilt:

$$E(Z) = E(X) + E(Y) \tag{6.3}$$

und

$$D^2(Z) = D^2(X) + D^2(Y) \tag{6.4}$$

Die Erweiterung auf mehr als zwei Zufallsvariablen ist offensichtlich.

---

[1]) Der Wert 1,645 gilt für ein 90%-Konfidenzintervall und ist bei anderen Konfidenzniveaus entsprechend zu modifizieren.

● Produkte logarithmisch normalverteilter Variablen

Das Produkt zweier oder mehrerer voneinander unabhängiger logarithmisch normalverteilter Variablen ist seinerseits logarithmisch normalverteilt.

Es ergibt sich im Falle der beiden Variablen X und Y für $Z = X \cdot Y$ eine logarithmische Normalverteilung mit folgenden Parametern:

$$E(Z) = E(X) \cdot E(Y) \tag{6.5}$$

und

$$\varepsilon_z^2 = \varepsilon_x^2 + \varepsilon_y^2 \tag{6.6}$$

Auch in diesem Falle ist die Erweiterung auf mehr als zwei Zufallsvariablen offensichtlich.

Die Ermittlung der Parameter für die Verteilung des Endergebnisses kann nun unter Benutzung der voranstehenden Beziehungen oder mit Hilfe von Monte-Carlo-Simulationen (/6-11/) erfolgen.

6.4.3.2 Unsicherheiten der erwarteten Häufigkeiten unerwünschter Ereignisse

● Nitrierer

Die erwartete Eintrittshäufigkeit für eine Explosion im Nitrierer liegt mit einer Wahrscheinlichkeit von 90 % zwischen den Werten

$$h_{05} = 8{,}7 \cdot 10^{-3}\ a^{-1} \text{ und } h_{95} = 0{,}1\ a^{-1}$$

Nach Durchführung der im vorangehenden Abschnitt vorgeschlagenen Verbesserungen ergeben sich die Konfidenzintervallgrenzen

$$h'_{05} = 3{,}6 \cdot 10^{-4}\ a^{-1} \text{ und } h'_{95} = 1{,}3 \cdot 10^{-2}\ a^{-1}$$

- Kocher

Die erwartete Eintrittshäufigkeit für eine Explosion im Kocher liegt mit einer Wahrscheinlichkeit von 90 % zwischen den Werten

$$h_{05} = 8{,}5 \cdot 10^{-3}\ a^{-1} \text{ und } h_{95} = 0{,}11\ a^{-1}$$

Die im vorangehenden Abschnitt vorgeschlagenen Verbesserungen führen auf 90 % Vertrauensgrenzen von

$$h'_{05} = 5{,}7 \cdot 10^{-4}\ a^{-1} \text{ und } h'_{95} = 1{,}5 \cdot 10^{-2}\ a^{-1}$$

- Hydraulisches Transportsystem

Die erwartete Eintrittshäufigkeit für ein Betriebsversagen des hydraulischen Transportsystems liegt mit einer Wahrscheinlichkeit von 90 % zwischen den Werten

$$h_{05} = 0{,}3\ a^{-1} \text{ und } h_{95} = 3{,}6\ a^{-1}$$

In allen Fällen darf als gesichert gelten, daß die Systemverbesserung real ist und nicht im Bereich der statistischen Unsicherheit liegt, da Mittelwerte und Fraktile der Verteilungen der Eintrittshäufigkeiten des unerwünschten Ereignisses für das verbesserte System unter den entsprechenden Werten für die ursprüngliche Auslegung liegen.

6.4.4 Schlußbemerkung

Die Untersuchung hat gezeigt, daß die Anwendung der Fehlerbaumanalyse auf eine Reihe nutzbringender Vorschläge zur Erhöhung der Anlagensicherheit geführt hat, die darüber hinaus - obwohl dies nicht das ausdrückliche Ziel der Analyse war - auch eine Erhöhung ihrer Verfügbarkeit bewirken. Manche Ergebnisse folgten bereits aus den qualitativen Überlegungen, die bei der Er-

arbeitung der Fehlerbäume angestellt wurden und sich daraus ergaben, daß die Art der Systembetrachtung bei der Fehlerbaumanalyse derjenigen des Anlagenkonstrukteurs entgegengesetzt ist. Werden beim Entwurf die Systeme vor allem unter dem Gesichtspunkt ihres Funktionierens betrachtet, so sucht man bei der Erstellung von Fehlerbäumen in systematischer Weise nach Versagensmöglichkeiten. Die Verbindung der beiden gegenläufigen Denkansätze führt dann auf Verbesserungen. Dies gilt offenbar auch dann, wenn - wie im vorliegenden Fall - bei der Auslegung der Anlage auf langjährige Betriebs- und Entwurfserfahrung zurückgegriffen werden kann.

Die Quantifizierung der Fehlerbäume brachte zusätzliche Einsichten und deckte Bereiche auf, in denen die Sicherheitsvorkehrungen unausgewogen waren. Die aus ihr abgeleiteten Vorschläge führen zu einer Reduzierung der Explosionshäufigkeiten um den Faktor 10 und lassen sich mit geringem technischen und finanziellen Aufwand verwirklichen. Einer Interpretation der Ergebnisse im absoluten Sinne steht jedoch der Mangel an geeigneten Zuverlässigkeitsdaten auf dem Gebiet chemischer Anlagen entgegen, der allzu häufig Schätzungen von Unsicherheitsfaktoren oder sogar Ausfallraten bedingte. Dies wird besonders deutlich bei der Behandlung des Transportsystems, in dem ein Flüssig-Feststoffgemisch gefördert wird. Für einen solchen Fall liegen überhaupt keine Beobachtungswerte vor. Zum Teil spiegelt sich die Unsicherheit bei den Zuverlässigkeitsdaten auch in den Konfidenzintervallen der Endergebnisse wider, bei denen die Ober- und Untergrenze sich durch Faktoren unterscheidet, die je nach behandeltem System zwischen 10 und 30 liegen. Andererseits läßt sich feststellen, daß unter den Komponenten wichtiger Systeme, wie beispielsweise der Regel- und Notablaßeinrichtungen von Nitrierer und Kocher, nur die Temperaturfühler und im letzteren Falle zusätzlich die Ablaßventile in typischer Weise durch chemische Substanzen belastet sind, während alle anderen Komponenten einer industrieüblichen Belastung ausgesetzt sind. Aus diesem Grund ist den zugehörigen numerischen Ergebnissen ausreichendes Vertrauen zu schenken.

Durch systematische Erhebungen von Zuverlässigkeitsdaten im Bereich chemischer Anlagen könnten die Probleme bei der Quantifizierung der Fehlerbäume gemindert und eine schärfere Eingrenzung der Endergebnisse erreicht werden.

Die Vorschläge zur Systemänderung wurden vom Anlagenhersteller und -betreiber angenommen. Sie sind zum Teil bereits verwirklicht.

7. SCHLUSSFOLGERUNGEN

Probabilistische Untersuchungen haben im Bereich der Chemie nicht die Bedeutung, die sie in anderen Sektoren wie beispielsweise der Kerntechnik erlangt haben. Vielmehr stehen dort qualitative Sicherheitsanalysen im Vordergrund. Diese dienen vor allem dem Auffinden störfallauslösender Ereignisse. Die dabei verwendeten Methoden benutzen Denkweisen, wie sie auch bei der Erstellung von Fehlerbäumen notwendig sind. Sie können beim Auffinden der logischen Zusammenhänge zwischen dem unerwünschten Ereignis und den Komponentenausfällen dienlich sein. Die Ergebnisse des qualitativen Teils der durchgeführten Fehlerbaumanalysen zeigen, daß auch bereits in dieser Phase der Untersuchung wertvolle Hinweise für eine Verbesserung der Anlage gewonnen werden können. Den Weg zu einem ausgewogenen Sicherheitskonzept weist in der Regel erst die quantitative Auswertung der Fehlerbäume. Wegen des Mangels an geeigneten Zuverlässigkeitsdaten auf dem Gebiet der Chemie sollten die Ergebnisse probabilistischer Untersuchungen derzeit jedoch nicht als Absolutwerte angesehen werden, sondern vorzugsweise dem Vergleich verschiedener Konstruktionsalternativen dienen. Sie können aber auch zur Beurteilung von Einzelsystemen mit wenig typisch chemisch belasteten Komponenten, wie beispielsweise den Regel- und Abschaltsystemen der in Kapitel 6 untersuchten Anlage, herangezogen werden.

Durch die Bereitstellung geeigneter Zuverlässigkeitsdaten aufgrund systematischer Auswertungen im Bereich der Chemie ließe

sich die Aussagekraft probabilistischer Analysen auf diesem Gebiet erhöhen und der Aufwand zu ihrer Erstellung erheblich vermindern.

Um zu entscheiden, welche Bereiche der chemischen Industrie vorzugsweise quantitativ untersucht werden sollten, wäre eine verstärkte Auswertung der Schadenserfahrung wünschenswert, damit Ergebnisse, wie sie im Kapitel 2 dargelegt wurden, besser abgesichert werden können.

Die Untersuchung der Anlage zur Herstellung von Hexogen hat gezeigt, daß die Fehlerbaumanalyse ein geeignetes Instrument zur Sicherheitsbeurteilung von Chemieanlagen sein kann. Die Übernahme der Verbesserungsvorschläge durch den Anlagenbetreiber bedeutet, daß der Ablauf der Analyse und die daraus abgeleiteten Schlußfolgerungen auch den Praktiker zu überzeugen vermochten.

SCHRIFTTUM

Kapitel 1:

/1-1/ Reactor Safety Study - An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants WASH-1400 (NUREG-75/014), October 1975

/1-2/ Gesellschaft für Reaktorsicherheit:
Deutsche Risikostudie Kernkraftwerke - Eine Untersuchung zu dem durch Störfälle in Kernkraftwerken verursachten Risiko - Hauptband -
Hrsg.: Der Bundesminister für Forschung und Technologie, Verlag TÜV Rheinland, Köln, 1979

/1-3/ Risk Analysis of Six Potentially Hazardous - Industrial Objects in the Rijnmond Area, A Pilot Study
A Report to the Rijnmond Public Authority, D. Reidel, Publishing Comp., Dordrecht, Boston, London, 1982

Kapitel 2:

/2-1/ Sax, N.I.:
Dangerous Properties of Industrial Materials
Verlag van Nostrand, Reinhold Comp., New York, Cincinnati, Toronto, London, Melbourne, 1975

/2-2/ Fire and Explosion Index: Hazard Classification Guide
5th Edition, Dow Chemical Company, Midland, Michigan, October 1980

/2-3/ Hommel, G.:
Handbuch der gefährlichen Güter
Springer-Verlag, Berlin, Heidelberg, 1980

/2-4/ Kier, B., und G. Müller:
Erweiterung der Störfalldatenbank und Erstellung des Handbuchs Störfälle
Umweltforschungsplan des BMI, Luftreinhaltung, Forschungsbericht 10409303, Mai 1983

/2-5/ Goldfarb, A.S., et al.:
Organic Chemicals Manufacturing Hazards
Science Publishers Inc., Ann Arbor, Michigan, 1981

Kapitel 3:

/3-1/ Fire and Explosion Index: Hazard Classification Guide
5th Edition, Dow Chemical Comp., Midland, Michigan, October 1980

/3-2/ Lewis, D.J.:
The Mond Fire, Explosion and Toxicity Index - A Development of the Dow Index -
A.I.Ch.E. Loss Prevention Symposium, Houston, 1979

/3-3/ Mieze, G.:
Vorläufige Gefahrenanalyse
Kerntechnik 9 (1971), S. 381-386

/3-4/ Balemans, A.W.M., et al.:
Checklist: Guidelines for Safe Design of Process Plants
1st International Loss Prevention Symposium, Delft, May 1974

/3-5/ Lawley, H.G.:
Operability Studies and Hazard Analysis
CEP, Vol. 70, No. 4 (1974), S. 45-60

/3-6/ A Guide to Hazard and Operability Studies
Chemical Industries Association Ltd., London, 1981

/3-7/ Der Störfall im chemischen Betrieb - Verhütung durch Prognose, Auffinden der Ursachen, Abschätzen der Auswirkungen, Gegenmaßnahmen (PAAG-Verfahren)
Berufsgenossenschaft der chemischen Industrie, Heidelberg, 1980

/3-8/ Lees, F.P.:
Loss Prevention in the Process Industries
Vol. I and II, Verlag Butherworths, London, 1980

/3-9/ DIN 25448:
Ausfalleffektanalyse
Beuth Verlag, Berlin, 1980

/3-10/ Daniels, J.T., und P.L. Holden:
Quantification of Risk
4th International Symposium on Loss Prevention and Safety Promotion in the Process Industries, EFCE Publication, Series Nr. 33, 1983

/3-11/ DIN 25419:
Teil 1: Störfallablaufanalyse - Störfallablaufdiagramm, Methode und Bildzeichen
Beuth Verlag, Berlin, 1977

/3-12/ Gesellschaft für Reaktorsicherheit:
Deutsche Risikostudie Kernkraftwerke; Fachband 1: Ereignisablaufanalyse
Hrsg.: Der Bundesminister für Forschung und Technologie, Verlag TÜV Rheinland, Köln, 1980

/3-13/ Gesellschaft für Reaktorsicherheit:
Deutsche Risikostudie Kernkraftwerke - Eine Untersuchung zu dem durch Störfälle in Kernkraftwerken verursachten Risiko
- Hauptband -
Hrsg.: Der Bundesminister für Forschung und Technologie, Verlag TÜV Rheinland, Köln, 1979

/3-14/ Hazardous Installations (Modification and Survey) Regulations 1978
H.M. Stationary Office, London, 1978

/3-15/ Putte van de, T., und F.H. Meppelder:
Identification of Major Hazard Installation in the Process Industries
3rd International Symposium on Loss Prevention and Safety Promotion in the Process Industries, Basel, 15.-19. September 1980

/3-16/ Risk Analysis of Six Potentially Hazardous - Industrial Objects in the Rijnmond Area, A Pilot Study
A Report of the Rijnmond Public Authority, D. Reidel, Publishing Comp., Dordrecht, Boston, London, 1982

/3-17/ Pyman, M.A.F., und T. Gjerstadt:
Experience in Applying Hazard Assessment; Techniques Offshore in the Norwegian Sector
4th International Symposium on Loss Prevention and Safety Promotion in the Process Industries, EFCE Publication, Series No. 33, 1983

/3-18/ Hough, B.:
Risk Assessment of Shipping Terminal Operations
4th International Symposium on Loss Prevention and Safety Promotion in the Process Industries, EFCE Publication, Series No. 33, 1983

/3-19/ Aldwinckle, D.S., und D.H. Slater:
Risk and Reliability Methods; Used in the Analysis of an Offshore LNG Liquefaction and Storage Ship
4th International Symposium on Loss Prevention and Safety Promotion in the Process Industries, EFCE Publication, Series No. 33, 1983

/3-20/ Jacobsen, O.F.:
Methodology Problems in Repredicting Accidents which have Actually Occurred
4th International Symposium on Loss Prevention and Safety Promotion in the Process Industries, EFCE Publication, Series No. 33, 1983

/3-21/ Haastrup, P.:
Design Error in the Chemical Industry
4th International Symposium on Loss Prevention and Safety Promotion in the Process Industries, EFCE Publication, Series No. 33, 1983

Kapitel 4:

/4-1/ Caldarola, L.:
Fault Tree Analysis with Multistate Components
KfK 2761, EUR 5756e, Karlsruhe, 1979

/4-2/ Caldarola, L.:
Generalized Fault Tree Analysis Combined with State Analysis
KfK 2530, EUR 5754e, Karlsruhe, 1980

/4-3/ Gesellschaft für Reaktorsicherheit:
Deutsche Risikostudie Kernkraftwerke; Fachband 2: Zuverlässigkeitsanalyse
Hrsg.: Der Bundesminister für Forschung und Technologie, Verlag TÜV Rheinland, Köln, 1981

/4-4/ Nielsen, D., O. Platz und H.E. Kongsø:
Reliability Analysis of a Proposed Instrument Air System
Risø-M-1903, Roskilde/Denmark, 1977

/4-5/ Hauptmanns, U.:
Fault Tree Analysis of a Proposed Ethylene Vaporization Unit
Ind. Eng. Chem. Fundam., Vol. 19, No. 3 (1980), S. 300-309

/4-6/ Hauptmanns, U., J. Yllera und H. Sastre:
Safety Analysis for the Ammonia-Air Mixing, System of a Plant for Production of Nitric Acid
Journal of Chemical Engineering of Japan, Vol. 15, No. 4 (1982), S. 286-291

/4-7/ Hauptmanns, U., und H. Sastre:
Safety Analysis of a Plant for the Production of Vinyl Acetate
Journal of Chemical Engineering of Japan, Vol. 17, No. 2, (1984), S. 165-173

/4-8/ Reactor Safety Study - An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants WASH-1400 (NUREG-75/014), October 1975

/4-9/ Gesellschaft für Reaktorsicherheit:
Deutsche Risikostudie Kernkraftwerke - Eine Untersuchung zu dem durch Störfälle in Kernkraftwerken verursachten Risiko
- Hauptband -
Hrsg.: Der Bundesminister für Forschung und Technologie, Verlag TÜV Rheinland, Köln, 1979

/4-10/ Risk Analysis of Six Potentially Harzardous - Industrial Objects in the Rijnmond Area, A Pilot Study
A Report to the Rijmond Public Authority, D. Reidel, Publishing Comp., Dordrecht, Boston, London, 1982

/4-11/ Barlow, R.E., und F. Proschan:
Statistical Theory of Reliability and Life Testing - Probability Models
Verlag Holt, Rinehart and Winston, New York, 1975

/4-12/ Kamarinopoulos, L.:
Anwendung von Monte-Carlo-Verfahren zur Ermittlung von Zuverlässigkeitsmerkmalen technischer Systeme
IRL-Bericht 14, Berlin, 1976

/4-13/ Güldner, W., et al.:
Programmsystem RALLY - Zur probabilistischen Sicherheitsbeurteilung großer technischer Systeme
GRS-44, Köln, 1982

/4-14/ Vesely, W.E., et al.:
Fault Tree Handbook
NUREG-0492 (1981), Hrsg.: NRC, Washington D.C.

Kapitel 5:

/5-1/ Gesellschaft für Reaktorsicherheit:
Deutsche Risikostudie Kernkraftwerke; Fachband 3: Zuverlässigkeitskenngrößen und Betriebserfahrungen
Hrsg.: Der Bundesminister für Forschung und Technologie, Verlag TÜV Rheinland, Köln, 1980

/5-2/ Gaede, K.-W.:
Zuverlässigkeit - Mathematische Modelle
Carl Hanser Verlag, München, Wien, 1977

/5-3/ Schneeweiss, W.:
Zuverlässigkeitstheorie
Springer-Verlag, Berlin, Heidelberg, New York, 1973

/5-4/ Risk Analysis of Six Potentially Hazardous - Industrial Objects in the Rijnmond Area, A Pilot Study
A Report to the Rijnmond Public Authority, D. Reidel, Publishing Comp., Dordrecht, Boston, London, 1982

/5-5/ Green, A.E., und A.J. Bourne:
Reliability Technology
Verlag Wiley-Interscience, London, New York, Sydney, Toronto, 1972

/5-6/ Anyakora, S.N., G.F.H. Engel und F.P. Lees:
Some Data on the Reliability of Instruments in the Chemical Plant Environment
The Chemical Engineer (1971), S. 396-402

/5-7/ Skala, V.:
Improving Instrument Service Factors
Instrumentation Technology (1974), S. 27-30

/5-8/ Gibson, M.R.:
Field Data from the Chemical Industry
Second National Reliability Conference, Birmingham, March 1979, 2B/2/1 - 2B/2/8

/5-9/ Hömke, P., C. Verstegen et al.:
Zuverlässigkeitskenngrößenermittlung im Kernkraftwerk Biblis-B; Ausfallraten und ihre Einflußgrößen
GRS-A-744, September 1982

/5-10/ Mai, E., et al.:
Untersuchung der Zuverlässigkeit von Druckabsicherungen in Kernkraftwerken
Forschungsbericht, BMI-Forschungsvorhaben RS II-510321/245 SR 214, Köln, September 1981

/5-11/ Meinlschmidt, G., und R. Schwaiger:
Ein Informationssystem zur Ermittlung von Zuverlässigkeitskenngrößen im Kernkraftwerk Biblis-B
GRS-A-560, Februar 1981

/5-12/ Hömke, P., und C. Verstegen:
Zuverlässigkeitskenngrößenermittlung im Kernkraftwerk Biblis-B
GRS-A-532, Dezember 1980

/5-13/ Hömke, P., C. Verstegen, W. Kutsch und H. Heer:
Erfahrungen bei der Grunddatenerfassung zur Ermittlung von Zuverlässigkeitskenngrößen im Kernkraftwerk Biblis-B
RWE-Bericht zum BMFT-Forschungsvorhaben RS-264, April 1981

/5-14/ Gesellschaft für Reaktorsicherheit:
Deutsche Risikostudie Kernkraftwerke; Fachband 2: Zuverlässigkeitsanalyse
Hrsg.: Der Bundesminister für Forschung und Technologie, Verlag TÜV Rheinland, Köln, 1981

/5-15/ Reactor Safety Study - An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plant WASH-1400 (NUREG-75/014), October 1975

/5-16/ Lewis, H.W., et al.:
Risk Assessment Review Group
Report to U.S. Nuclear Regulatory Commission, Washington D.C., September 1978, NUREG/CR-0400

/5-17/ Fleming, Raabe, Hannaman, et al.:
HTGR Accident Initiation and Progression Analysis
Status Report, Vol. II: AIPA Risk Assessment Methodology,
GA-A 13617, October 1975

/5-18/ Hörtner, H.:
Problems of Failure Data with Respect to Systems; Reliability Analysis
Nuclear Engineering and Design 71 (1982), S. 387-389

/5-19/ Vesely, H.:
Estimating Common Cause Failure Probabilities in Reliability and Risk Analyses: Marshall-Olkin-Specializations
Proceedings of the International Conference on Nuclear System Reliability Engineering and Risk Assessment, Gatlinburg, Tennessee, June 1977, ed. by J.B. Fussel and G.R. Burdick, Society for Industrial and Applied Mathematics, Philadelphia, 1977, S. 314-341

/5-20/ Atwood, C.L.:
Estimators for the Binominal Failure Rate Common Cause Model
NUREG/CR-1401, EGG-EA-5112, NRC, Washington D.C., April 1980

/5-21/ Swain A.D., und H.E. Guttmann:
Handbook of Human Reliability - Analysis with Emphasis on Nuclear Power Plant Applications; Final Report
U.S. Nuclear Regulatory Commission, Washington D.C., 1983, NUREG/CR-1278

/5-22/ Hacker, W.:
Allgemeine Arbeits- und Ingenieurpsychologie
Verlag Huber, Bern, Stuttgart, Wien, 1978

Kapitel 6:

/6-1/ Urbanski, T.:
Chemistry and Technology of Explosives
Pergamon Press, Oxford, New York, 1965-1967

/6-2/ Lingens, P., et al.:
Sprengstoffe
in: Ullmanns Encyklopädie der technischen Chemie, Bd. 21, Weinheim, 1982

/6-3/ Berthmann, A.:
Explosivstoffe
in: W. Winnacker und L. Küchler (Hrsg.): Chemische Technologie - Organische Technologie III, Carl Hanser Verlag, München, 1972

/6-4/ Sax, N.I.:
Dangerous Properties of Industrial Materials
Verlag: Van Nostrand Reinhold Comp., New York, Cincinnati, Toronto, London, Melbourne, 1975

/6-5/ Meyer, R.:
Explosivstoffe
Verlag Chemie, Weinheim, New York, 1976

/6-6/ Anyakora, S.N., G.F.H. Engel und F.P. Less:
Some Data on the Reliability of Instruments in the Chemical Plant Environment
The Chemical Engineer (1971), S. 396-402

/6-7/ Swain, A.D., und H.E. Guttmann:
Handbook of Human Reliability - Analysis with Emphasis on Nuclear Power Plant Applications; Final Report
U.S. Nuclear Regulatory Commission, Washington D.C., 1983
NUREG/CR-1278

/6-8/ Green, A.E., und A.J. Bourne:
Reliability Technology
Verlag Wiley-Interscience, London, New York, Sydney, Toronto, 1972

/6-9/ Skala, V.:
Improving Instrument Service Factors
Instrumentation Technology (1974), S. 27-30

/6-10/ Gesellschaft für Reaktorsicherheit:
Deutsche Risikostudie Kernkraftwerke; Fachband 3: Zuverlässigkeitskenngrößen und Betriebserfahrungen
Hrsg.: Der Bundesminister für Forschung und Technologie, Verlag TÜV Rheinland, Köln, 1980

/6-11/ Gesellschaft für Reaktorsicherheit:
Deutsche Risikostudie Kernkraftwerke; Fachband 2: Zuverlässigkeitsanalyse
Hrsg.: Der Bundesminister für Forschung und Technologie, Verlag TÜV Rheinland, Köln, 1981

Gesellschaft für Reaktorsicherheit (GRS) mbH

Schwertnergasse 1
5000 Köln 1

Forschungsgelände
8046 Garching

ISBN 3-923875-07-X